Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Counternetwork Operations

A Monograph
by
MAJ Derek Jones
USA

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

AY 2009

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
30-04-2009	SAMS Monograph	JUL 2008 – MAY 2009

4. TITLE AND SUBTITLE
Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Counternetwork Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ Derek Jones, USA

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies (SAMS)
250 Gibbons Avenue
Fort Leavenworth, KS 66027-2134

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Since the events of September 11, 2001 the United States military counternetwork operations, theory, and doctrine have failed to account for the form, function, and logic of clandestine cellular networks used by both interstate insurgencies, such as those in Iraq and Afghanistan, as well as by global insurgencies, like al Qaeda and its associated movements. The failure to understand the form, function, and logic of clandestine cellular networks has led to the incorrect application of counternetwork theories. Counternetwork operations specifically targeting key leaders, facilitators, individuals with special skills, or highly connected individuals, intuitively seem to be the correct targets for disconnecting clandestine cellular networks. However, there has been little comparative analysis done to verify if these operations are in fact having the overall effect required to disrupt, neutralize, defeat, or ultimately destroy these networks.

Understanding the form, function, and logic of clandestine cellular networks reveals that the removal of single individuals, regardless of function, is well within the tolerance of this type of organizational structure and thus has little long-term effect. At the same time, highly connected nodes violate the principles of clandestine operations since they are obviously highly visible when compared to a competent clandestine practitioner that does not want a discernable signature in order to remain hidden from the counterinsurgent. Thus, by focusing on the highly connected individuals as high priority targets, US efforts have effectively "culled the herd" of poor clandestine practitioners. These two examples provide the two most common errors in the current counternetwork theories and operations, and the errors are all due to a lack of a systemic understanding of clandestine cellular networks.

This monograph uses a modified process-trace methodology to analyze the form, function, and logic of clandestine cellular networks in order to dispel the myths associated with current network and counternetwork theories, and challenge the contemporary thoughts on counternetwork operations. This work concludes with the development of six principles of clandestine cellular networks, along with a myriad of conclusion based on the analysis of the form, function, and logic of these networks, to provide a deeper understanding of clandestine cellular networks. Understanding the form, function, and logic of clandestine cellular networks is the first step to more effective counternetwork operations. **SDG**

15. SUBJECT TERMS
Clandestine cellular networks, insurgent networks, terrorist networks, counternetwork operations, information age networks.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Stefan J. Banach, U.S. Army
(U)	(U)	(U)	(U)	118	**19b. PHONE NUMBER** *(include area code)* 913-758-3302

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

MAJ Derek Jones

Title of Monograph: Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Counternetwork Operations

Approved by:

_____ Monograph Director
Daniel G. Cox, Ph.D

_____ Reader
Jeffrey J. Goble, COL, SF

_____ Reader
Alexander J. Ryan, Ph.D

_____ Director, School of Advanced Military Studies
Stefan J. Banach, COL, IN

_____ Director, Graduate Degree Programs
Robert F. Bauman, Ph.D

Abstract

Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Counternetwork Operations by MAJ Derek Jones, 118 pages.

Since the events of September 11, 2001 the United States military counternetwork operations, theory, and doctrine have failed to account for the form, function, and logic of clandestine cellular networks used by both interstate insurgencies, such as those in Iraq and Afghanistan, as well as by global insurgencies, like al Qaeda and its associated movements. The failure to understand the form, function, and logic of clandestine cellular networks has led to the incorrect application of counternetwork theories. Counternetwork operations specifically targeting key leaders, facilitators, individuals with special skills, or highly connected individuals, intuitively seem to be the correct targets for disconnecting clandestine cellular networks. However, there has been little comparative analysis done to verify if these operations are in fact having the overall effect required to disrupt, neutralize, defeat, or ultimately destroy these networks.

Understanding the form, function, and logic of clandestine cellular networks reveals that the removal of single individuals, regardless of function, is well within the tolerance of this type of organizational structure and thus has little long-term effect. At the same time, highly connected nodes violate the principles of clandestine operations since they are obviously highly visible when compared to a competent clandestine practitioner that does not want a discernable signature in order to remain hidden from the counterinsurgent. Thus, by focusing on the highly connected individuals as high priority targets, US efforts have effectively "culled the herd" of poor clandestine practitioners. These two examples provide the two most common errors in the current counternetwork theories and operations, and the errors are all due to a lack of a systemic understanding of clandestine cellular networks.

This monograph uses a modified process-trace methodology to analyze the form, function, and logic of clandestine cellular networks in order to dispel the myths associated with current network and counternetwork theories, and challenge the contemporary thoughts on counternetwork operations. This work concludes with the development of six principles of clandestine cellular networks, along with a myriad of conclusion based on the analysis of the form, function, and logic of these networks, to provide a deeper understanding of clandestine cellular networks. Understanding the form, function, and logic of clandestine cellular networks is the first step to more effective counternetwork operations.

TABLE OF CONTENTS

Introduction

> Design of effective countermeasures depends on first understanding undergrounds.[1]
>
> Andrew R. Molnar, et. al. (1963)

> It's hard for us to fight the cells because they're many different leaders, different thought processes, it's not like a normal enemy we fight, it's not structured.[2]
>
> U.S. Army Intelligence Officer, Iraq (2006)

> I'm not sure we really understood how embedded Al Qaeda was becoming.... Al Qaeda in Iraq has proved to be a very resourceful enemy, capable of regenerating at a time when we thought it didn't have that capability.[3]
>
> U.S. Army Battalion Commander, Iraq (2009)

Since the events of September 11, 2001 the United States military counternetwork operations, theory, and doctrine have failed to account for the form, function, and logic of clandestine cellular networks used by both interstate insurgencies, such as those in Iraq and Afghanistan, as well as by global insurgencies like al Qaeda and its associated movements. The failure to understand the form, function, and logic of clandestine cellular networks has led to the incorrect application of counternetwork theories.[4] Counternetwork operations specifically

---

[1] Andrew R. Molnar, William A Lybrand, Lorna Hahn, James L. Kirkman, and Peter B. Riddleberger, *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare*, (Washington, DC: Special Operations Research Office, November 1963), http://handle.dtic.mil/100.2/AD436353 [accessed on December 21, 2008], v.

[2] Greg Grant, "Insurgency Chess Match: Allies Match Wits, Tactics with Ever-Changing Enemy in Iraq," *Defense News* (February 27, 2006), 6.

[3] Associated Press Corps, "Iraqi Forces Weary of America's Troop Withdrawal," *Fox News* Web site (March 09, 2009), http://www.foxnews.com/story/0,2933,507544,00.html [accessed March 9, 2009].

[4] The form, function, and logic construct used in this monograph is derived from Edward PW Hayward, *Planning Beyond Tactics: Towards a Military Application of the Philosophy of Design in the Formulation of Strategy*, (master's thesis, Fort Leavenworth, KS, 2008), http://usacac.army.mil/cac2/

targeting key leaders, facilitators, individuals with special skills, or highly connected individuals, intuitively seem to be the correct targets for disconnecting clandestine cellular networks.[5] However, there has been little comparative analysis done to verify if these operations are in fact having the overall effect required to disrupt, neutralize, defeat, or ultimately destroy these networks.[6] Understanding the form, function, and logic of clandestine cellular networks reveals that the removal of single individuals, regardless of function, is well within the tolerance of this type of organizational structure and thus has little long-term effect, as has been noted when a high-value individual or target (HVI or HVT), such as when Abu Musab Zarqawi, the al Qaeda

---

SAMS/ HaywardMonograph-PhilosophyofDesign.pdf [accessed on March 2, 2009], 1. Hayward uses "*Form*, *Function* and *Logic* [author's emphasis] as a method of reducing the existential crisis between what we expect to happen…and what we actually experience." Hayward's use of form, function, and logic is derived from Gilles Deleuze and Felix Guattari, *A Thousand Plateaus; Capitalism and Schizophreni*, (Minneapolis: University of Minnesota Press, 1987); As Molnar, et. al., explain, "the emphasis in the study is on describing the functions and techniques of undergrounds." Molnar, et. al., 27.

[5] For example, author David C. Gompert noted in 2007, "[Counterinsurgency] operations could be improved by understanding and addressing the forms of networking that characterize the global insurgency. As mentioned earlier, recent works at RAND reveal the significance of jihadist 'nodes, hubs, and cores,' the first being fighters, terrorists, and other operatives; the second being the tier responsible for planning, financial operations, communications, material support, and providing direction to the nodes; and the third being the theoreticians and charismatic leaders. While a great deal of attention has been given to nodes and cores, this ongoing RAND work highlights the advantage of targeting *hubs*—the middle tiers that are critical to enabling nodes to turn ideological guidance of the cores into action." David C. Gompert, *Heads We Win: The Cognitive Side of Counterinsurgency (COIN)*, (Santa Monica, CA: RAND Corporation, 2007), http://www.rand.org/pubs/occasional_papers/2007/RAND_OP168.pdf [accessed on March 4, 2009], 48-49; Also, The National Security Council noted, "The loss of a leader can degrade a [terrorist] group's cohesiveness and in some cases may trigger its collapse." National Security Council, *National Strategy for Combating Terrorism*, (Washington, D.C.: The White House, 2006), http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/nss2006.pdf [accessed April 6, 2009], 12. For information on facilitators, see Anthony H. Cordesman, *Iraq's Sunni Insurgents: Looking Beyond Al Qa'ida*, (working draft, Washington, D.C.: Center for Strategic and International Studies, July 16, 2007), http://www.csis.org/media/csis/pubs/070716_sunni_insurgents.pdf [accessed on February 8, 2009], 2.

[6] As author Linda Robinson notes, "Special Operations units…stepped up their already intense pace to target…Al-Qaeda's top three tiers of leaders, financiers, bomb-makers, and facilitators. The Al-Qaeda in Iraq (AQI) organization had proven its ability to regenerate almost as fast as the commandos captured or killed its leaders." Linda Robinson, *Tell Me How This Ends*, (New York, NY: PublicAffairs, 2008), 56-7, 180.

leader in Iraq, was killed in 2006.[7] At the time, there was speculation that this strike would end the insurgency or at least seriously degrade the insurgency.[8] However, it had little overall effect.[9] At the same time, highly connected nodes violate the principles of clandestine operations since they are obviously highly visible when compared to a competent clandestine practitioner that does not want a discernable signature in order to remain hidden from the counterinsurgent. Thus, by focusing on the highly connected individuals as high priority targets, US efforts have effectively "culled the herd" of poor clandestine practitioners, while further educating the competent clandestine practitioners on US counternetwork methods. This also allows other poor clandestine practitioners, those that may have been lucky enough to survive their incompetence, but were smart enough to learn from those not so fortunate, to adapt, and increase their competence in the application of the clandestine arts.[10] These two examples, high value

---

[7] Jeffrey White, *An Adaptive Insurgency: Confronting Adversary Networks in Iraq*, Policy Focus #58, (Washington, D.C.: The Washington Institute for Near East Policy, September 2006), http://www.washingtoninstitute.org/pubPDFs/PolicyFocus58.pdf [accessed March 23, 2009], 8.

[8] Bob Woodward, *The War Within: A Secret White House History 2006-2008*, (New York, NY: Simon & Schuster, 2008), 59.

[9] Ibid., 131. Other studies on targeting insurgent leaders have concluded that removing key leaders has limited long-term effect; for example, see Lisa Langdon, Alexander J. Sarapu, and Matthew Wells, "Targeting the leadership of terrorist and insurgent movements: Historical Lessons for Contemporary Policy Makers," *Journal of Public and International Affairs* 15, (Spring 2004): 73-76, http://www.princeton.edu/~jpia/pdf2004/Chapter%204.pdf [accessed on 23 March 2009]; Graham H. Turbiville, Jr., *Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations: Selected Perspectives and Experience*, Joint Special Operations University Report 07-6, (Hurlburt Field, FL: Joint Special Operations University, June 2007), http://jsoupublic.socom.mil/publications/jsou/JSOU07-6turbivilleHuntingLeadershipTargets_final.pdf [accessed on November 22, 2008], 1, 75-79; and Daniel Byman, *The Five Front War: The Better Way to Fight Global Jihad*, (Hoboken, NJ: John Wiley & Sons, 2008), 116-119, under "The Rewards and Costs of Targeted Killing."

[10] For example, RAND analysts Seth Jones and Martin Libicki explain, "A network is vulnerable, however, at its hubs. If enough hubs are destroyed, the network breaks down into isolated, noncommunicating islands of nodes. Hubs in a social network are vulnerable because most communications go through them. With good intelligence, law-enforcement authorities should be able to identify and arrest these hubs." Seth G. Jones and Martin C. Libicki, *How Terrorist Groups End: Lessons from Countering al Qa'ida*, (Santa Monica, CA: RAND Corporation, 2008), http://www.rand.org/pubs/

individuals and highly connected individuals, provide the two most common types of errors in the current counternetwork theories and operations, and the errors are all due to a lack of a systemic understanding of clandestine cellular networks.

Current attack methodologies, such as the kill or capture of high-value individuals or targets, are largely based on theories that clandestine cellular networks are like any network and can be defeated by removing key nodes to delink the network.[11] What emerged with the events of 9/11, and has now become readily accepted by counternetwork theorists and practitioners alike, is the idea that the clandestine cellular networks used by adversaries like al Qaeda and the insurgents in Iraq and Afghanistan, are "information-age networks."[12] Theorists describe these adversary networks as highly connected, flat, leaderless, agile, and adaptive, mirroring today's business networks or social networks like those found on the internet.[13] Mark Buchanan, author of *Nexus*, explains, "Since the attacks, we have become accustomed to the idea that the West is

---

monographs/2008/RAND_MG741-1.pdf [accessed on March 23, 2009], 126; also see Byman, 94; under "Darwinian process."

[11] Turbiville, 1-2, 9.

[12] For example, noted terrorism expert Bruce Hoffman explains, "It is therefore possible that the insurgency in Iraq may indeed represent a new form of warfare for a new, networked century. It is too soon to determine whether this development, involving loose networks of combatants who come together for a discrete purpose only to quickly disperse upon its achievement, will prove to be a lasting or completely ephemeral characteristic of postmodern insurgency;" Bruce Hoffman, *Insurgency and Counterinsurgency in Iraq*, (Santa Monica, CA: RAND Corporation, 2004), http://www.rand.org/pubs/occasional_papers/ 2005/RAND_OP127.pdf [accessed on November 22, 2008], 18; Department of the Army, FM 3-24, *Counterinsurgency*, (Washington, D.C.: U.S. Government Printing Office, December 2006), http://usacac.army.mil/cac2/Repository/Materials/COIN-FM3-24.pdf [accessed on January 15, 2009], 1-4.

[13] For instance, see: Hoffman, *Insurgency*,18; David Ronfeldt, "Al Qaeda and its affiliates: A global tribe waging segmental warfare?" First Monday 10, no. 3 (March 7, 2005), under "Abstract," http://firstmonday.org/issues/ issue10_3/ronfeldt/index.html [accessed on March 4, 2009]; Mark Buchanan, *Nexus: Small Worlds and the Groundbreaking Science of Networks*, (New York, NY: W. W. Norton & Company, 2002), 21; John Arquilla and David Ronfeldt, *Networks and Netwars*, (Santa Monica, CA: RAND, 2001), http://www.rand.org/pubs/ monograph_reports/MR1382/index.html [accessed on January 30, 2009], 6-16; Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century*, (Philadelphia, PA: University of Pennsylvania Press, 2008), 144; Marc Sageman, *Understanding Terror Networks*, (Philadelphia, PA: University of Pennsylvania Press, 2004), 137.

battling against a decentralized 'network of terrorists cells' [sic] that lacks any hierarchical command structure and is distributed throughout the world. This network seems to be a human analogue of the Internet, with an organic structure that makes it extremely difficult to attack."[14] However, as this monograph will show, clandestine cellular networks are not information-age networks, and despite the West's desire to mirror-image information-age networks onto insurgent and terrorist networks, the form, function, and logic of clandestine cellular networks are very different.[15] Clandestine cellular networks provide a means of survival, both in form, through their cellular or compartmentalized structure, and in function, through the use of clandestine arts or tradecraft to minimize the signature of the organization—all based on the logic that the primary concern is that the movement needs to survive to attain its political goals. The old adage that the insurgent wins by not losing is the fundamental driving force behind why insurgencies, and any organization conducting nefarious activities that could lead to being killed or captured by a government's security forces, use this type of organizational structure.

Organizational structure, in this case, clandestine cellular networks, and how they are established, grow, and operate, as well as the logic behind the organizational structure, plays a large role in the overall success of an insurgency.[16] Yet the importance of organization as a

---

[14] Buchanan, 21.

[15] As Molnar, et. al., found, "Undergrounds have been the base of resistance and revolutionary movements throughout recorded history;" and that "it is clear that clandestine organizations are not the product of a particular political or religious ideology; cultural, ethnic, national, or geographic grouping of persons; structure or form of government; segment of society or social class; or stage of a society's economic or technological development. Also [sic] it is clear that undergrounds are not new nor unique to the contemporary world scene, although such an impression is easily created by the pressure of current problems. Underground movements directed toward changes in governing authority have appeared in societal life throughout recorded history." Molnar, et. al., 4, 23-26.

[16] Roger Trinquier had a similar opinion based on his experiences in Algeria, explaining, "In seeking a solution, it is essential to realize that in *modern warfare* we are not up against just a few armed bands spread across a given territory, but rather against an *armed clandestine organization* whose essential

dynamic of insurgency is often overlooked or misunderstood by counterinsurgent theorists and practitioners. This is especially true when it comes to clandestine cellular networks.[17] Current US counterinsurgency doctrine found in FM 3-24, *Counterinsurgency*, provides only one dedicated paragraph on the role and "interplay" of organization in insurgency and one paragraph on clandestine networks.[18] FM 3-24 notes, "Networked organizations…have a limited ability to attain strategic success because they cannot easily muster and focus power."[19] Although this statement is not backed up by evidence in the manual, it is apparent that since 9/11 and in most historical cases of insurgency, the underground and auxiliary members extensively used clandestine cellular networks as their organizational method to protect their core leadership,

---

role is to impose its will upon the population. Victory will be obtained only through the complete destruction of that organization. This is the master concept that must guide us in our study of *modern warfare*." Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency*, (London: Pall Mall Press, 1964), http://cgsc.leavenworth.army.mil/carl/resources/csi/trinquier/trinquier.asp [accessed January 15, 2009], 8-9.

[17] The Special Operations Research Office (SORO) conducted the last major studies on undergrounds during Vietnam; see Molnar, et. al. The most notable US effort to lethally counter insurgent undergrounds was the Phoenix Program in Vietnam. As author Charles Simpson explains "the concept was to identify and then capture or kill members of the Vietcong political or support personnel living undercover in disputed villages, or even in so-called pacified areas;" Charles M. Simpson III, *Inside the Green Berets: The First Thirty Years*, (Novato, CA: Presidio Press, 1983), 9; also see Dale Andrade, *Ashes to Ashes: The Phoenix Program and the Vietnam War*, (Lexington, MA: Lexington Books, 1990); Ken Tovo, "From the Ashes of the Phoenix: Lessons for Contemporary Counterinsurgency Operations," in *Strategic Challenges for Counterinsurgency and the Global War on Terrorism*, ed. Williamson Murray, (Carlisle, PA: Strategic Studies Institute, September 2006), http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB710.pdf [accessed on March 5, 2009], 17-42; United States Military Assistance Command, *PHUNG HOANG Advisors Handbook*, (Vietnam: United States Military Assistance Command, November 20, 1970), http://www.virtual.vietnam.ttu.edu/cgi-bin/starfetch.exe? cjGDEhjqEBDExu9fCcjH5b3O7 WlKcAYxLC5Cpx3X@ VJlyYEeHvEd5qSH NUIJ43IL6ur4w9KL5Vs J2XIamvRZF wD1ESf@ IDwdrC4x8S60DoE/ 1370406001.pdf [accessed on March 25, 2009].

[18] FM 3-24, see paragraph 1-70, page 1-13, and paragraph 1-95, page 1-17, organization and networks, respectively; Appendix B describes the use of social network analysis to map insurgent networks, but provides no other organizational analysis or information on clandestine cellular networks.

[19] Ibid., 1-17; despite this statement, paragraph 1-87, page 1-16, states that "contemporary insurgencies often develop in urban environments, leveraging formal and informal networks for action. Understanding these networks is vital to defeating such insurgencies."

intelligence, logistics support, and some lethal operational capabilities.[20] For insurgents in hostile or non-permissive environments, where there is a large government security presence or an unsympathetic population, especially in urban areas, clandestine cellular networks become the primary organizational structure.[21]

US counterinsurgency operations and doctrine have always tended to focus on the military aspects of the insurgency, the guerrillas, since they are overt, and understandable from a military point of view.[22] The underground and auxiliary, and their use of clandestine cellular

[20] For this monograph, Molnar's, et. al., definition of undergrounds is used: "Clandestine organizational elements of politico-military movements attempting to illegally weaken, modify, or replace the existing governing authority." Molnar, et. al., 13-15, 27. The author's definition of auxiliary is used and defined here as the active civilian support mechanism for the insurgency which conducts clandestine activities, such as logistics, intelligence, and operational support. For current examples of undergrounds, see David G. Fivecoat and Aaron T. Schwengler, "Revisiting *Modern Warfare*: Counterinsurgency in the Mada'in Qada," *Military Review* (November-December 2008), http://usacac.army.mil/CAC2/ MilitaryReview/Archives/English/MilitaryReview_20081231_art012.pdf [accessed on March 2, 2009], 79; Fivecoat and Schwengler contrasted the Shi'a extremist militia organization with a clandestine Algerian cell structure from Trinquier's *Modern Warfare*, stating, "The Shi'a organization replicated the configuration Trinquier fought in Algeria in the late 1950s. This order of battle chart proved a valuable tool." Also see Shahid Afsar, Chris Samples, and Thomas Wood, "The Taliban: An Organizational Analysis," *Military Review* (May-June 2008), http://usacac.army.mil/CAC/milreview/ English/MayJun08/ SamplesEngMayJun08.pdf [accessed on March 3, 2009], 65-67. The authors note that the Taliban is a networked organization, with, "Specialized departments at the Taliban's top and middle tiers," including specialized "departments" based on skills. At the lower levels, the Taliban operates more like a rural guerrilla army, but the authors describe these as "village cells" of "between 10 and 50 part-time fighters."

[21] FM 3-24, 1-7, 1-13, 1-16, 1-17, and 1-23; Molnar, et. al., 13-15.

[22] FM 3-24, 1-17; Department of the Army, FM 90-8, *Counterguerrilla Operations*, (Washington, D.C.: U.S. Government Printing Office, August 1986), 1-5. As FM 90-8 notes, "Counterguerrilla operations are geared to the active military elements of the insurgent movement only;" 1-5. Guerrilla warfare expert Virgil Ney shows this propensity of western counterinsurgency theories is to focus on the overt fighting forces of the insurgents has remained largely unchanged in the last fifty years, as he noted in 1961, "Western military writers have considered guerrilla warfare almost exclusively in purely military terms. They have been concerned primarily with the effectiveness of guerrilla tactics when employed against conventional armies;" Virgil Ney, *Guerrilla War: Principles and Practices*, (Washington, D.C.: Command Publications, 1961), 20; also, Trinquier identified this problem in Algeria, "[Operational commanders] have little interest in the less noble task, however essential, of subtle work with the population that enables guerrilla bands to survive despite local defeats the forces of order periodically inflict." Trinquier, 58; and Momboisse notes, "The importance of the underground is tremendous. Indeed without it the Revolution would not succeed. Unfortunately its importance is often ignored or greatly

networks, have never been completely understood, and have always been minimized in their role in insurgency because they remained hidden. However, as the diagram in figure 1 shows, historically, the overt guerrilla elements only make up the tip of the proverbial insurgency iceberg when compared to the underground and auxiliary.[23] In much the same way, a conventional

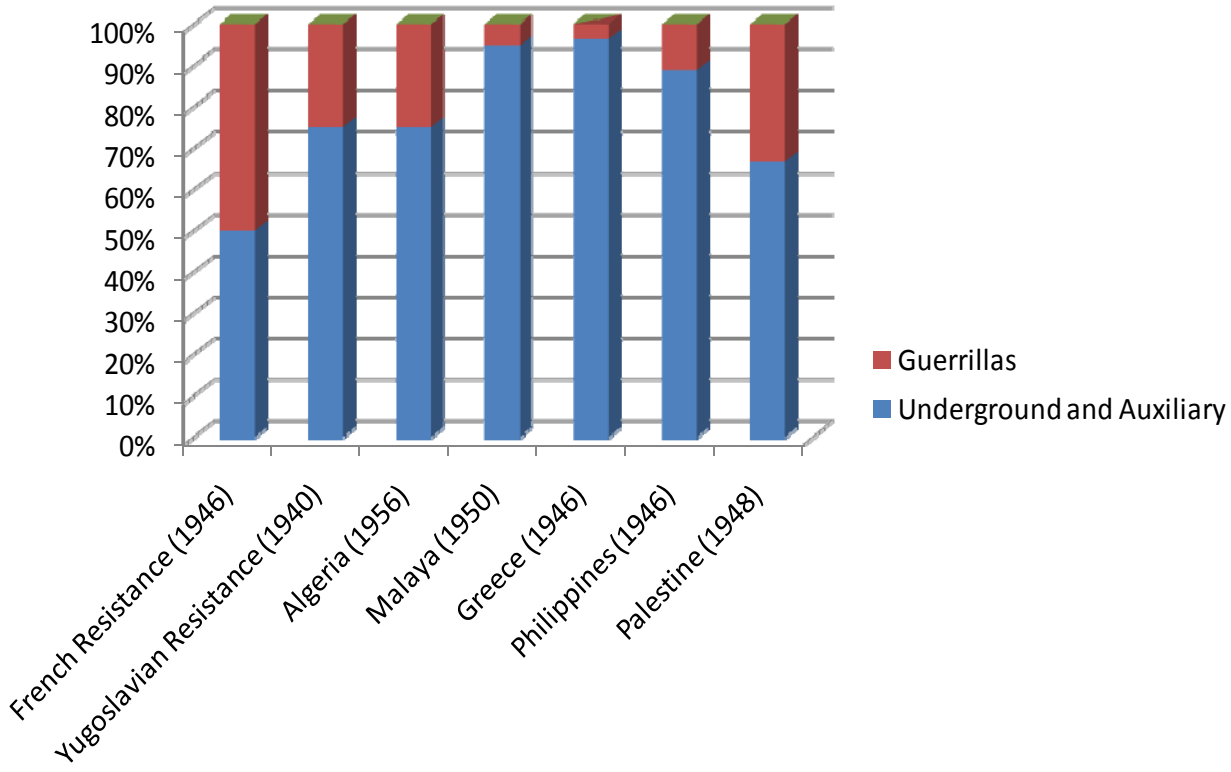

Figure 1. Historical Guerrilla to Underground and Auxiliary Ratios[24]

military's ground forces' have a disproportionate number of combat forces to non-combat forces,

---

underrated…unquestionably due to the secrecy of its operation." Raymond M. Momboisse, *Blueprint of Revolution: The Rebel, The Party, The Technique of Revolt*, (Springfield, IL: Charles C Thomas, 1970), 62.

[23] Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, and Peacekeeping*, (St. Petersburg, FL: Hailer Publishing, no date), 68; Molnar, et. al., 14-15.

[24] Figure 1 is based on data from Molnar, et. al., 14-15.

often referred to as the "tooth-to-tail ratio."[25] For the US military, this ratio is generally 1:4, combat to non-combat, with the combat forces at the tip.[26] Based on the data presented in figure 1, the average ratio is one guerrilla for every nine underground and auxiliary members.[27] Like conventional military organizations, an insurgent organizations require significant non-combat support, including command and control, intelligence, logistics, and information, to support the overt combat elements of an insurgency. As highlighted by the above statement from FM 3-24, networks are unable to "muster and focus combat power," doctrine fails to account for the asymmetry of insurgency: it is not about combat power, it is about overall effect by maintaining pressure over time—the proverbial "war of the flea"—versus a decisive battle.[28]

The insurgency in Iraq, which has been primarily an underground urban insurgency is consistent with this. Every time the insurgents held ground or massed, such as in Fallujah, the conventional forces could generally deal them a decisive blow; decisive only in the sense that for a short time, they were defeated. Constant coalition casualties from improvised explosive devices, small-arms fire from hit-and-run cells in urban areas, and snipers began to wear down US public support and political will—arguably the US center of gravity. It could also be argued that the

---

[25] John J. McGrath, *The Other End of the Spear: The Tooth-to-Tail Ratio (T3R) in Modern Military Operations*, The Long War Series Occasional Paper 23, (Fort Leavenworth, KS: Combat Studies Institute Press, 2007), 2.

[26] Ibid., 88.

[27] Molnar, et. al., 13.

[28] FM 3-24, 1-17; John J. McCuen, The *Art of Counter-Revolutionary War*, (St. Petersburg, FL: Hailer Publishing, 2005), 51; As guerrilla warfare expert Robert Taber explains, "Analogically, the guerrilla fights the war of the flea, and his military enemy suffers the dog's disadvantage: too much to defend; too small, ubiquitous, and agile an enemy to come to grips with. If the war continues long enough—this is the theory—the dog succumbs to exhaustion and anemia without ever having found anything on which to close his jaws or to rake with his claws." Robert Taber, *The War of the Flea: A Study of Guerrilla Warfare Theory and Practice*, (New York, NY: Lyle Stuart, Inc., 1965), 27-28.

Shi'a insurgency, with the help of Iran, was generally a clandestine insurgency that successfully stayed under the US radar, except for overt Shi'a elements, like Muqtada al Sadr's Madhi Army and Iranian-backed Special Groups using explosively formed penetrators (EFP).[29] Thus, failure to understand the form, function, and logic of clandestine cellular networks used by undergrounds and urban guerrillas has hampered US counterinsurgency efforts.[30] With increased urbanization throughout the world, urban insurgencies will be the primary means of insurgency, shifting away from rural insurgencies as the primary methods of the past, setting the stage for greater use of clandestine cellular networks.

The importance of organization has not been lost in current and past Army Special Operations Forces (ARSOF) doctrine, especially within its unconventional warfare and foreign internal defense doctrines, in which "organization" is one of the "seven dynamics of insurgency;" an analytical tool used by ARSOF to understand the form, function, and logic of insurgent movements.[31] The seven dynamics have been determined to be common to most insurgencies, and, "provide a framework for analysis that can reveal the insurgency's strengths and weaknesses."[32] The other six dynamics are: leadership, ideology, objectives, environment and geography, external support, phasing and timing.[33] The current FM 3-24 also uses "dynamics of

---

[29] Robinson, 11, 161-168; and Alireza Jafarzadeh, *The Iran Threat: President Ahmadinejad and the Coming Nuclear Crisis*, (New York, NY: Palgrave MacMillan, 2007), 81-87, 113-114, 116-119.

[30] FM 3-24, 1-17; Grant, 6; and Associated Press Corps.

[31] Department of the Army, Field Manual 3-05.201, *Special Forces Unconventional Warfare Operations*, (Washington, D.C.: US Government Printings Office, April 30, 2003), 1-5. This version of the ARSOF UW manual is used instead of the current FM 3-05.201 due to the upgrade in classification of the current manual; see also, Department of the Army, Field Manual 31-20-3, *Foreign Internal Defense: Tactics, Techniques, and Procedures for Special Forces*, (Washington, D.C.: US Government Printings Office, September 20, 1994), 1-7 to 1-10.

[32] FM 3-05.201, 1-5.

[33] Ibid., 1-5 to 1-8.

insurgency," but has dropped organization, and thus only has six dynamics—leadership, objectives, ideology and narrative, environment and geography, external support and sanctuary, and phasing and timing.[34] Although pieces and parts of the insurgent organization are discussed throughout the manual, the organizational role and importance is lost. Yet, the importance of organization is readily apparent when reading past theorists, such as Galula, Kitson, McCuen, Ney, Thompson, and Trinquier, all of which devoted numerous pages to describe the organization, including clandestine cellular networks, not just as parts, but the parts as the whole, and the whole within the context of the other dynamics of insurgency.[35] Trinquier went so far as to note, "In seeking a solution [to insurgency], it is essential to realize that in *modern warfare* we are not up against just a few armed bands spread across a given territory, but rather against an *armed clandestine organization*."[36] Trinquier further highlights, "Victory will be obtained only through the complete destruction of that organization. This is the master concept that must guide us in our study of *modern warfare*."[37]

The significance of organization has also not been lost on "modern" theorists. For example, famed insurgency and terrorism expert Bard E. O'Neill dedicates a chapter in his book *Insurgency & Terrorism* to the subject, while his contemporaries, noted experts Bruce Hoffman

---

[34] FM 3-24, 1-13 to 1-17.

[35] David Galula, *Counterinsurgency Warfare: Theory and Practice*, (St. Petersburg, FL: Hailer Publishing, 2005), 43-58; Kitson, 32-48, 128; McCuen, 30-37; Ney, 17-20, 44-46; Robert Thompson, *Defeating Communist Insurgency: Experiences from Malaya and Vietnam*, (London: Chatto&Windus, 1974), 28-42; and Trinquier, 10-15.

[36] Trinquier, 9.

[37] Ibid.

and John Arquilla have presented testimony to Congress on the organizational characteristic and function of al Qaeda.[38] As O'Neill explains,

> No analysis of an insurgency will be complete or meaningful if it fails to address the scope, complexity, and cohesion of the insurgent movement. A careful look at the structures and workings of insurgent political and military organizations can reveal a good deal about the progress of an insurrection, as well as the type and magnitude of the threat confronting the government.[39]

Although it is apparent that the importance of "organization" has not been lost on the theorists, the theorists' understanding of the form, function, and logic of clandestine cellular networks is less apparent or completely lacking.[40] Although theorists and practitioners regularly use phrases

---

[38] Bard E. O'Neill, *Insurgency & Terrorism: From Revolution to Apocalypse*, 2nd ed., (Washington, DC: Potomac Books, 2005), Chapter 6; Bruce Hoffman, "Combating Al Qaeda and the Militant Islamic Threat," testimony presented to the House Armed Service Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities, February 16, 2009, (Santa Monica, CA: RAND Corporation, 2006), http://www.rand.org/ pubs/testimonies/2006/ RAND_CT255.pdf [Accessed January 15, 2009], 3-6; John Arquilla, "It Takes a Network: On Countering Terrorism While Reforming the Military," testimony before the House Armed Service Subcommittee on Terrorism, Unconventional Threats and Capabilities, (September 18, 2008), http://armedservices.house.gov/pdfs/TUTC091808/ Arquilla_Testimony091808.pdf [accessed on November 22, 2008], 1.

[39] O'Neill, 134-135.

[40] Gompert, 48-49; Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, (New York, NY: Penguin Group, 2006), 5; Also, Sageman explains, "Where a small-world network is vulnerable to targeted attack is at its hubs. If enough hubs are destroyed, the network breaks down into isolated, noncommunicating islands of nodes." Sageman, *Understanding*, 140. Arquilla noted in his congressional testimony that the U.S. is in what he calls, "an 'organizational race' to build networks [and]….The terrorists remain on their feet and fighting, in large part because their nimble, networked structures have been given the opportunity to keep developing, their hallmarks being the decentralization of authority, the proliferation of small cells throughout the world, and an abundance of lateral links – many in cyberspace – among and between their many nodes." Arquilla, 1. Authors Michele Zanini and Sean Edwards explain, "What has been emerging in the business world is now becoming apparent in the organizational structures of the newer and more active terrorist groups, which appear to be adopting decentralized, flexible network structures. The rise of the networked arrangements in terrorist organization is part of a wider move away from the formally organized…groups." Michele Zanini and Sean J.A. Edwards, "The Networking of Terror in the Information Age," in *Networks and Netwars*, ed. John Arquilla and David Ronfeldt, (Santa Monica, CA: RAND, 2001), http://www.rand.org/pubs/ monograph_reports/MR1382/index.html [accessed on January 30, 2009], 32. Also, Sageman applies information age theories in his book, *Understanding Terror Network*, explaining, "In more formal language, growth of this [terrorist] network was not a random process but one of preferential attachment, meaning that the probability that a new node will connect to any given node is *proportional to the number*

like “covert networks,” “terrorist networks,” and “undergrounds,” they rarely codify what is meant by the description. In most cases, as will be shown in this work, they do not understand or underestimate the significance of the terms, using them more as contemporary buzzwords than as technical terms.

---

of its existing links [author’s emphasis-further violating the principles of clandestine arts]….a small-world network resists fragmentation because of its dense interconnectedness… Hubs in social networks are vulnerable…law enforcement authorities should be able to identify and arrest these human hubs. This strategy has already shown *considerable success* [author’s emphasis].” Sageman, *Understanding*, 139-141.

As theorists Peter Holme, et. al., note, “None of the network models shows a behavior very similar to the real-world networks….This clearly suggests that there are other structures contributing to the network behavior during vertex attack, and conclusions from model networks should be cautiously generalized to real-world situations.” Petter Holme, Boem Jun Kim, Chang No Yoon, and Seung Kee Han, “Attack vulnerability of complex networks,” *Physical Review* E 65 (2002): 12, http://nlsc.ustc.edu.cn/ BJKim/PAPER/ PhysRevE_65_056109%20Attack%20 vulnerability%20of%20complex%20networks.pdf [accessed January 30, 2009]. Note theorist Stephen Borgatti focused on identifying key players within terrorist networks for attack with three goals,”(a) identifying nodes whose deletion would maximally fragment the network, (b) identifying nodes that, based on structural position alone, are potentially ‘in the know’, [sic] and (c) identifying nodes that are in a position to influence others.” Stephen P. Borgatti, “Identifying Sets of Structurally Key Players,” (lecture, Carnegie Mellon University Center for Computational Analysis of Social and Organizational Systems (CASOS), June 21, 2002), http://www.casos.cs.cmu.edu/publications/papers/ CASOSConf_2002_Day1.pdf [accessed November 22, 2008], 69; and Jonathan David Farley, “Breaking Al Qaeda Cells: A Mathematical Analysis of Counterterrorism Operations (A Guide for Risk Assessment and Decision Making),” *Studies in Conflict & Terrorism* 26, no. 26 (June 2003), 409. Farley attempts to develop a technique for determining the degree that a terrorist cell functions, to identify “when a battle against Al Qaeda has been won.” Although interesting, it shows the confusion of terms between cells and networks. He also falsely believes that his theory can successfully neutralize a cell or network by cutting the leadership off from the cell members.

For an examples of theorists that are beginning to identify weaknesses in network attack models, see: renowned social network theorist, Kathleen Carley, who notes, “Many are stepping forward suggesting that to understand [covert] networks we just need to ‘connect the dots’ and then isolate ‘key actors…in the network;’’ Carley further explains that attacking key actors “does not contend with the most pressing problem – the underlying network is dynamic. Just because you isolate a key actor…today…does not mean that the network will be destabilized and unable to respond.” see Kathleen M. Carley, *Estimating Vulnerabilities in Large Covert Networks*, (Pittsburgh, PA: Carnegie Mellon University, Institute for Software Research International, June 2004), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA466095& Location=U2&doc=GetTRDoc.pdf [accessed November 22, 2008], 2; and see Maksim Tsvetovat and Kathleen M. Carley, “Bouncing Back: Recovery Mechanisms of Covert Networks,” (paper presented at the *NAACSOS Conference 2003*, Day 3, Pittsburgh, PA, June 2003), http://www. casos.cs.cmu.edu/ publications/papers/tsvetovat_2003_ bouncingback.pdf [accessed November 22, 2008], ii.

Joint Publication 1-02 defines clandestine, as, "An operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor."[41] The 1960s-era Special Operations Research Office (SORO) noted, "Clandestine operations are those whose existence is concealed, because the mere observation of them betrays their illegal and subversive nature. Secrecy depends upon the skill in hiding the operation and rendering it invisible."[42] Clandestine art or tradecraft is used to conceal individual actions, but also to conceal organizational functions, such as information and intelligence sharing, lethal and non-lethal operations, logistical support, and linkages to overt elements of the movement such as political wings or guerrillas.[43] "Clandestine," the adjective, describes the function of the network, while "cellular" describes the form or structure of the network. Both form and function help define the logic of these types of networks and the elements within the insurgency that use them.

Reviewing historic works and documents on clandestine operations in insurgency and espionage, it becomes apparent that the form, function, and logic of clandestine cellular networks have largely remained unchanged.[44] Although some theorists might speculate that the

---

[41] Department of Defense, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, (Washington, D.C.: Government Printing Office, amended October 1, 2008), http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf [accessed on November 22, 2008], 91.

[42] Department of the Army, Pamphlet No. 550-104, *Human Factors Considerations of Undergrounds in Insurgencies*, (Washington, DC: Headquarters, Department of the Army, September 1966), http://cgsc.cdmhost.com/cgi-bin/showfile.exe?CISOROOT=/p4013coll9&CISOPTR=85 [accessed on November 22, 2008], 101.

[43] Fred Burton defines tradecraft as "the set of skills needed to conduct clandestine activities in a hostile environment without discovery." Fred Burton, "Beware of 'Kramer': Tradecraft and the New Jihadists," *STRATFOR* (January 19, 2006), http://www.stratfor.com/beware_kramer_tradecraft_and_new_jihadists [accessed on November 16, 2008], under title.

[44] The literature on undergrounds and clandestine operations varies. The most accessible for the Western reader are numerous accounts of clandestine operations from American and British World War II (WWII) veterans that served, in the British Special Operations Executive (SOE), the American Office of Strategic Services (OSS)—the precursor to the Central Intelligence Agency (CIA), including M. R. D. Foot, *SOE: The Special Operations Executive 1940-1946*, (n.p.: University Publications of America, Inc.,

information-age caused a revolutionary change allowing for the rise of global non-state actors and thus an adaptation to clandestine networks form, function, and logic, there is no evidence this has happened. Organizational use of clandestine cellular or compartmented networks (form) and the application of clandestine arts or tradecraft methods (function) have remained largely unchanged, having *evolved* to take advantage of the new technology, but not in a revolutionary way. Information technology, while increasing the rate and volume of information exchange, has also increased the risk to clandestine operations due to the increase in electronic and cyber-signature, which puts these types of communications into a realm that governments, like the US, can apply their technological advantage to indentify, monitor, track, and exploit. Thus, despite the power of the internet, and other information-age electronic devices, clandestine operators continue to use old clandestine methods and, in some cases, adapt them for use with the new technology.[45] In

---

1986); Will Irwin, *The Jedburghs: The Secret History of the Allied Special Forces, France 1944*, (New York, NY: Public Affairs, 2005); and Russell Miller, *Behind The Lines: The Oral History of Special Operations in World War II*, (New York, NY: New American Library, 2002). Author Sherri Greene Ottis provides an outstanding history of the escape and evasion lines in WWII occupied France, including the clandestine techniques, cellular networks, and German counternetwork operations, in *Silent Heroes: Downed Airmen and the French Underground*, (Lexington, KY: The University Press of Kentucky, 2001).

For informative works on undergrounds, including two by the Special Operations Research Office, see: DA PAM 550-104; Raymond M. Momboisse, *Blueprint of Revolution: The Rebel, The Party, The Technique of Revolt*, (Springfield, IL: Charles C Thomas, 1970); H. von Dach Bern, *Total Resistance: Swiss Army Guide to Guerrilla Warfare and Underground Operations*, ed. R. K. Brown, (Boulder, CO: Panther Publications, Inc., 1965); and Trinquier.

Espionage related works that provide extensive background on clandestine techniques include: Richard M. Bennett, *Espionage: Spies and Secret*, (London: Virgin Books Ltd, 2003); Alexander Orlov, *Handbook of Intelligence and Guerrilla Warfare*, (Ann Arbor, MI: The University of Michigan Press, 1965); I.E. Prikhodko, *Characteristics of Agent Communications and of Agent Handling in the United States of America*, (San Francisco, CA: Interservice Publishing Company, Inc., 1981); Roy Godson, *Dirty Tricks or Trump Cards: U.S. Covert Action & Counterintelligence*, (New Brunswick, NJ: Transaction Publishers, 2004); Allen W. Dulles, *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World*, (Guilford, CT: The Lyons Press, 2006); and Lindsay Moran, *Blowing My Cover: My life as a CIA Spy*, (New York, NY: Penguin Group, 2005).

[45] See Mark Owen, *A Discussion of Covert Channels and Steganography*, (n.p.: SANS Institute, March 19, 2002), http://www.sans.org/reading_room/whitepapers/covert/a_discussion_of_ covert_channels_and_steganography_678?show=678.php&cat=covert [accessed on March 5, 2009], 1;

fact, because they have to apply tradecraft, it slows their rate of communication down, thus denying the information-age theorists the monolithic information-aged networked enemy that they have portrayed since 9/11.

Other differences noted in clandestine literature is the scale of the different types of clandestine operations, from small networks of individuals conducting espionage, to insurgent movements utilizing clandestine cellular networks countrywide or globally. It is also interesting to note that based on the review of historical and current US, British, Soviet, Swiss, Iraqi, Iranian, and al Qaeda clandestine tactics, techniques, procedures, and principles, there is a broad commonality amongst these different actor's clandestine theories and practices. The greatest difference is not in the operational application, since they all use almost identical methods, but surprisingly in vocabulary and professionalism. The bottom line is that clandestine cellular networks, regardless of the environment, the country of origin, the clandestine background of the practitioner, or the clandestine task—lethal operations, logistics, or intelligence gathering—they all generally have the same form, function, and logic.

Patrick Di Justo, "How Al-Qaida Site Was Hijacked." *WIRED*, (August 10, 2002), http://www.wired.com/culture/lifestyle/news/2002/08/54455 [accessed March 7, 2009]; and Jim Wingate, *The Perfect Deaddrop: The Use of Cyberspace for Covert Communications*, (West Virginia: Steganography Analysis and Research Center (SARC), n.d.), http://www.infosec-technologies.com/steganograph.pdf [accessed January 31, 2009], 2. Also a history of US spy Robert Hanssen notes, "Hanssen and his Russian intelligence handlers used simple, time-honored tradecraft to communicate with each other….Although Hanssen had substantial communications with the KGB about using sophisticated computer techniques for communications, they used no sophisticated communications devices or modern technology but relied on the US postal service, the telephone, and signal sites and deaddrops." *A Counterintelligence Reader*. Edited by Frank J. Rafalko. http://www.fas.org/ irp/ops/ ci/docs/index.html [accessed March 25, 2009], 102.

Methodology

This monograph will answer the primary research question, "what is the form, function, and logic of clandestine networks?" A modified process-trace methodology will be used to develop principles of clandestine cellular networks based on an analysis of clandestine theories, histories, and operations.[46] These principles can then be used by the counterinsurgent to better understand the clandestine cellular networks used by interstate and global insurgencies. The monograph is organized into four main sections—form, function and logic, followed by the principles of clandestine operations that emerge the previous three sections. An additional appendix provides further information on the specific types of clandestine networks—indigenous or external and professional or non-professional—likely to be encountered in a complex insurgency with multiple actors, as well as explaining the concept of the inherent "clandestine potential" of an indigenous population.

This monograph will specifically focus on the organizational dynamic of insurgency to gain an understanding the organizational form, function, and logic of insurgents' use of clandestine cellular networks. First, the *form* of clandestine networks will initially be explained with respect to how this organizational structure fits within the broader context of insurgency, then how these cellular networks are structured. The discussion on form will analyze the organizational structure, including size or scale, down to the cell level, and will focus on the key

[46] For background on the process-trace methodology, see Andrew Bennett and Alexander L. George, "Process Tracing in Case Study Research," (paper presented at the MacArthur Foundation Workshop on Case Study Methods, Harvard University, Cambridge, MA, October 17-19, 1997), http://users.polisci.wisc.edu/kritzer/teaching/ps816/ProcessTracing.htm [accessed on October 15, 2008]; and Tulia G. Falleti, "Theory-Guided Process-Tracing in Comparative Politics: Something Old, Something New," *Newsletter of the Organized Section in Comparative Politics of the American Political Science Association* 17, no. 1 (Winter 2006): 9-14, http://www.polisci.upenn.edu/~falleti/Falleti-CP-APSANewsletter06-TGPT.pdf [accessed on November 28, 2008].

element of form for clandestine cellular networks—compartmentalization. Second, this work will explain how clandestine cellular networks *function* through the application of clandestine arts or tradecraft and reinforce the form of the organization, while most importantly explaining how insurgents use the clandestine arts or tradecraft to maintain a low signature. Lastly, the form and function will be synthesized to explain the *logic* behind the use of clandestine cellular networks by elements of insurgencies, both intrastate and global, which have an overall goal of ensuring the organization survives to reach its political goal. This final section will further explain the pressures faced by members of clandestine organizations. From this form, function, and logic analysis, a set of principles will be developed that capture the essence of clandestine cellular networks which can be used as a test of network theories.

Form of Clandestine Cellular Networks

One definition of form is "the shape or structure of something."[47] Clandestine elements of an insurgency use form—organization and structure—for compartmentalization, relying on the basic network building block, the compartmented cell, from which the term "cellular" is derived.[48] Structural compartmentalization at all levels ideally isolates breaches in security to a single cell, and even better, to a single individual. Cellular structure ensures that a single strike does not lead to the compromise of the entire network, with only those individuals with direct linkages and knowledge being at risk. As Soviet defector Alexander Orlov explains, "the majority of the agents who take part in the same operation should not know one another, should not meet, and should not know each other's addresses. The idea behind [this] was, [sic] that if a man does

[47] As defined on Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/form%5B1%5D [accessed on February 16, 2009].

[48] DA PAM 550-104, 19.

not know something he will not be able to divulge it."[49] To understand the organizational significance of clandestine cellular networks, it is important to understand the context in which different components of the insurgency use this type of organizational structure.

Components of an Insurgency

The Army Special Operations Forces' (ARSOF) doctrine uses a three-component model of insurgency consisting of the underground, the auxiliary, and the guerrillas.[50] The underground and auxiliary are the primary components that utilize clandestine cellular networks. The underground is responsible for the overall command, control, communications, information, subversion, intelligence, and clandestine direct action operations—such as terrorism, assassination, and intimidation.[51] The original members and core of the insurgency generally operate as members of the underground. The auxiliary is the clandestine support mechanism, directed by the underground, that provides logistics, operational support, and intelligence collection.[52] The direct action elements of the underground operate in the grey area between clandestine and overt operations—having direct lethal interaction with the counterinsurgent or target audience in the case of terrorism—thus increasing the risk of detection. These elements,

---

[49] Orlov, 152.

[50] FM 3-05.130, 4-6 to 4-8; FM 3-24, 1-11 and 1-12. FM 3-24 dropped this construct and opted for broader five-component model consisting of movement leaders, combatants, political cadre, auxiliaries, and the mass base; the ARSOF three-component model is focused on the active supporters to the insurgency. Largely beyond the scope of this monograph, there is a fourth component, the mass support base, but these are generally the passive elements that support the insurgency or are neutral. This components will only be discussed here as a pool of possible recruits for the growth of the movement or replacement for movement members that are killed or captured, thus moving from passive support to active support and into one of the three components. In the three-component model, the first component to develop in an insurgency is the underground.

[51] DA PAM 550-104, 1; FM 3-05.201, 3-31 to 3-34; and Molnar, et. al., 23-29.

[52] FM 3-05.201, 3-24 to 3-30; and Molnar, et. al., 28.

often referred to as "urban guerrillas," operate in cells of three to ten members, all having direct interactions between individuals of the cell. This interaction increases the signature and inherent risk of the cell and individuals with direct links if a member is identified by the counterinsurgents. However, the underground leadership mitigates this risk through compartmentalization between the direct action cells and the rest of the network. Also, these types of cell members have limited training and are generally easy to replace. Their vulnerability and recuperability—ability to be replaced—has earned them the nom de guerre "low hanging fruit."[53]

The third and last major component is the guerrillas—the overt arm of the insurgency.[54] The size and organizational structure of guerrilla elements are dependent on their environment—rural guerrillas are generally more hierarchical in structure, along normal military lines, while as noted above, urban guerrillas operate using clandestine cellular networks. In rural insurgencies, the guerillas may be small guerrilla bands or near-conventional guerrilla armies made up of thousands, and may even have modern heavy weapons, such as tanks and artillery.[55] However, urban insurgencies, or combined rural and urban insurgencies, where the rural environment is not conducive to concealing or supporting large overt guerrilla units, such as the desert environment

---

[53] Roger Roy observes, "The brothers [suspected Afghan insurgents] shook hands with the Americans, and the soldiers filed out of the compound empty-handed, facing the tough truth about their job here: The foolish and the foolhardy among the insurgents—the low-hanging fruit on the terrorist tree—have, like the apples in [one of the brother's] orchard, already been plucked. Those who have survived this long won't be easy to catch." Roger Roy, "Tracking down Afghan insurgents like a "chess game" for U.S. troops," *The Seattle Times*, November 28, 2005, under "Fruitless Search," http://seattletimes.nwsource.com/cgi-bin/PrintStory.pl?document_id=2002650678& zsection_id= 2002107549&slug=afghanenemy28& date=20051128 [accessed on March 19, 2009];

[54] FM 3-05.201, 1-1, 3-18 to 3-24.

[55] The Northern Alliance in Afghanistan prior to 9/11 is a good example of a near-peer guerrilla army in the war-of-movement phase against the forces of the Taliban government.

of Iraq, are inherently more clandestine than overt.[56] In both cases, the clandestine elements of the insurgency resort to clandestine cellular networks as their organizational framework for operational security in the high threat environments. If guerrilla units are able to grow to large sizes, and become a near-peer competitor in a war-of-movement phase of an insurgency, the counterinsurgent is unable to effectively counter them, and thus, there is little need for compartmentalization or signature reduction.[57] At this overt end of the organizational scale, the units are operating with maximum efficiency and low security. At the other end of the scale, as Valdis Krebs notes, "covert networks trade efficiency for secrecy."[58]

The Development and Growth of Clandestine Cellular Networks

To understand the form of clandestine cellular networks it is important to understand how they develop and grow. The ARSOF model of Mao Tse-Tung's Protracted War Theory explains how an insurgency develops and matures. The ARSOF model consists of the latent and incipient phase, guerrilla warfare phase, and war-of-movement phase.[59] During the latent and incipient phase, the core organizes into clandestine cellular networks around a common goal based on an ideology and/or grievance, to establish the underground. The underground develops an auxiliary, and starts conducting non-violent subversion, such as demonstrations, walk-outs, and strikes, and

---

[56] FM 3-24, 1-7.

[57] FM 3-05.201, 1-8. War-of-movement phase is the final phase when an insurgency transitions from guerrilla warfare to conventional warfare.

[58] See Valdis E. Krebs, "Uncloaking Terrorist Networks," *First Monday* 7, no. 4 (April 1, 2002), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/941/863 [accessed on November 22, 2008].

[59] FM 3-05.201, 1-7 to 1-8. Mao's three phases are the strategic defensive, the strategic stalemate, and the strategic counteroffensive; FM 3-24, 1-6; other theorists, such as John McCuen uses a four phased model: organization, terrorism, guerrilla warfare, and mobile warfare, giving terrorism its own phase; McCuen, 40.

types of non-lethal sabotage of key infrastructure or factories causing production slowdowns.[60] This non-violent action then transitions to violent political action in the form of terrorism, intimidation, and coercion.[61] As the movement begins to develop and the security situation is at a level that overt elements can operate with some freedom of action, then the movement develops guerrilla units as its overt fighting force.

This transition into the guerrilla warfare phase, where overt attacks increase with the introduction of more conventionally organized guerrillas, marks the point where the underground is sufficiently large and robust enough to not only support an overt element, but recover if the overt element suffers losses. Even though the insurgency has moved into guerrilla warfare phase, the underground continues to operate and grow in order to gain resources, grow into new target areas, and build shadow government elements. In some cases, the establishment of shadow government elements takes place under the noses of the counterinsurgents, if there is poor population control, or the underground can wait until areas are liberated by its own guerrilla force, and then establish the shadow government. If successful, the guerrillas become near-peer military competitors with the government forces and begin the war-of-movement phase until successful or pushed back to a preceding phase. Although this model is an outstanding one for the overall movement, or what John McCuen calls "strategic phases," DA PAM 550-104 provides a five-phased model that provides sub-phases for the underground elements.[62]

---

[60] Momboisse, Chapters 17-20.

[61] Ibid., Chapters 21 and 22.

[62] DA PAM 550-104, 2; McCuen, 40. McCuen also uses a similar sub-phase model as well for undergrounds based on a French model referred to as "Trotsky's Five Phases of Revolution;" 42.

The first three phases of the 550-104 model take place in the latent and incipient phase of the protracted war phasing. In phase one, "*the clandestine organization phase*," the core organizes the clandestine cellular networks.[63] Phase two, the "*subversion and psychological offensive*," includes non-violent subversion, such as spreading rumors, strikes, boycotts, demonstrations, and limited terrorism.[64] Phase three, the "*expansion phase*," begins the transition from clandestine cellular networks to the development of guerrilla units, with phase four, the "*militarization phase*," marking the introduction of overt guerrilla forces.[65] The fifth phase of underground growth, and really the steady state for the underground until success or failure, is "*the consolidation phase*," in which the underground movement creates shadow governments, including meeting humanitarian, legal, security, religious, and education needs, as well as collecting taxes, or other resources and manpower from the population.[66] The underground uses its shadow government to establish control of areas, and as it name implies, it could be in parallel with current government programs. The intent in this final phase is to gain and maintain control of the human terrain—the population. The underground will continue to spread its control, almost a reverse of the oil-spot counterinsurgency strategy, to starve the government of support.[67]

---

[63] DA PAM 550-104, 2; and Momboisse, Chapter 4.

[64] DA PAM 550-104, 2; and Momboisse, 157, 220, 223-233, 238, 247, 262.

[65] DA PAM 550-104, 2-3.

[66] Ibid., 3.

[67] For information on oil spot theory see Robert J. Ward, "Oil Spot: Spreading Security to Counter Insurgency," *Special Warfare* 20, no.2 (March-April 2007): 8-17. http://www.soc.mil/swcs/swmag/07Mar.pdf [accessed on March 2, 2009]; "In 1954 General Challe introduced the 'spot-of-oil' strategy in an effort to pacify the Algerians." Molnar, et. al., 169.

Elements of Insurgent Clandestine Cellular Networks

The underground, as its name implies, begins with the core leadership and cadres that develop the ideology, find a common grievance to garner popular support, and develop a strategy and organizational pattern based on the physical, human, and security environments. The organizational structure of the underground is based on the clandestine cellular network model, with different cells assigned functions. These functions, as shown in the notional network in figure 2, include: leadership, logistics support, intelligence collection, counterintelligence, recruiting, training, finances, information operations, direct action (terrorism, assassination, kidnapping, sabotage, etc) cells, evasion networks, shadow government or overt political wings, and command and control of the other two elements, the auxiliary and the guerrillas. The core networks primarily operate within urban areas, with networks that extend to rural areas and provide support in conjunction with the auxiliary.[68] Underground elements operate almost entirely clandestinely, with a few exceptions being the overt political wings, shadow governments, and the direct action cells. Although there may be no visible link between the overt and clandestine elements from the perspective of the outside observer, there are likely strong ties, with the true leaders being hidden within the clandestine network providing guidance and direction to the representatives in the political wings and shadow governments.[69]

[68] FM 3-05.130, 4-7 to 4-8.

[69] See Thompson, 28-30; Trinquier, 10-13; and Galula, 44-48.

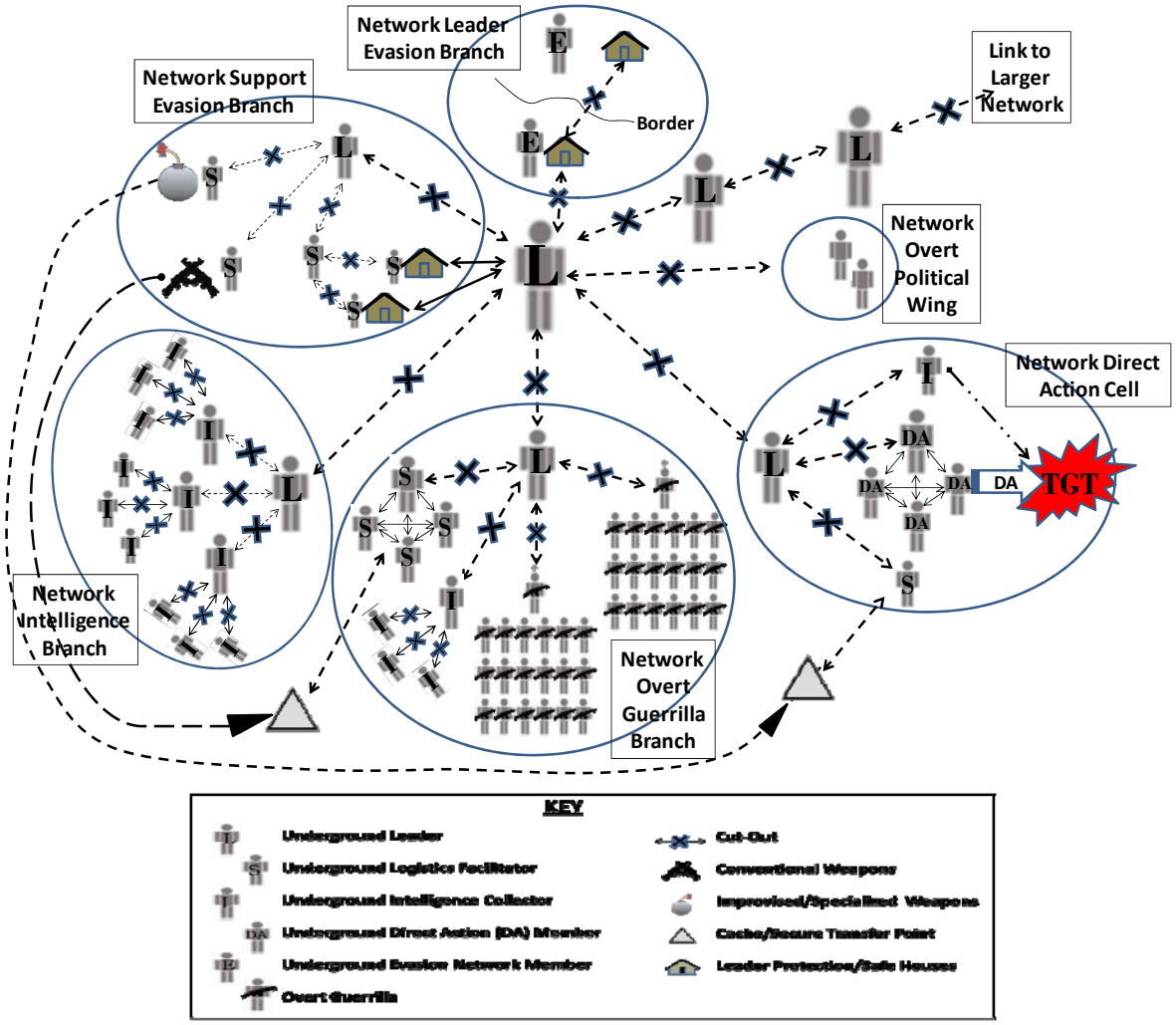

Figure 2. Example Insurgent Network[70]

[70] Figure based on the author's experiences and network diagrams from the following: Grant, 6; Kitson, 68,128; Molnar, et. al., 54, 204, 273, 300, and 319; DA PAM 550-104, 21-26; Trinquier, 11; Malcolm W. Nance, *Terrorist Recognition Handbook: Practitioner's Manual for Predicting and Identifying Terrorist Activities*, 2nd ed., (Boca Raton, FL: CRC Press, Taylor & Francis Group, 2008), 75-79; Thompson, 31; Bern, 86-89; Fivecoat and Schwengler, 79; Afsar, Samples, and Wood, 65-67. The authors note that the Taliban is a networked organization, with, "Specialized departments at the Taliban's top and middle tiers," including specialized "departments" based on skills. At the lower levels, the Taliban

As noted in figure 2, the clandestine cellular network is based on the core building block, the cell. The cell size can differ significantly from one to any number of members, as well as the type of interaction within the cell, depending on the function of cell. There are generally three functions—operations, intelligence, and support.[71] The cell members may not know each other, such as in an intelligence cell, with the cell leader being the only connection between the other members (see figure 3).[72] In more active operational cells, such as a direct-action cell, all the members are connected, know each other, perhaps are friends or are related, and conduct military-style operations that require large amounts of communications (see figure 3).[73] Two or more cells linked to a common leader are referred to as branches or sub-networks of a larger network, as shown in figure 2. Cells linked to a common leader are also referred to as "cells-in-parallel" or "cells-in-series" (see figure 4).[74] For example, operational cells may be supported by

---

operates more like a rural guerrilla army, but the authors describe these as "village cells" of "between 10 and 50 part-time fighters."

[71] DA PAM 550-104, 2, 19-26.

[72] Ibid., 20-23; see Figure 2 on page 22.

[73] Ibid., 20-21.

[74] Ibid., 20-26.

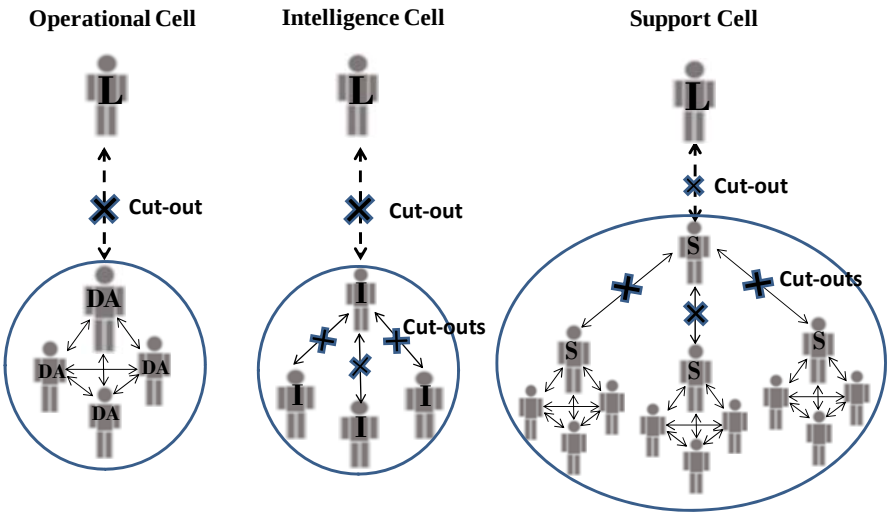

Figure 3. Examples of Functional Cells--Operational, Intelligence, Support[75]

an intelligence cell or logistics cell, or as shown in figure 4, the other cell-in-parallel could have the same operational function, and is available to the branch leader if the primary cell is interdicted.[76] If the cells within the branch are compartmented from each other, but have a role or function that builds on the other, they are referred to as "cells-in-series," with the branch leader coordinating their actions (see figure 4). Cells-in-series are primarily for manufacturing, safe-house networks, evasion networks, or weapons procurement and emplacement.[77]

---

[75] Based on functional cell figures 1-3, DA PAM 550-104, 21-23.

[76] Ibid., 24-25.

[77] A contemporary example of cell-in-series is an improvised explosive device (IED) branch or sub-network, in which the branch leader coordinates the actions of his different cells. The individual cells have no knowledge of the role or identity of the other cells within series. Thus, the branch leader directs his intelligence cell to identify a specific type of security forces vehicle to target and to develop its operational pattern. Another cell may build the appropriate IED, and place it in a cache. Simultaneously the cell's intelligence collector determines the most likely route that vehicle takes and builds the vehicles pattern of movement to determine the best time and location to interdict the target. Once the location for the IED ambush has been identified, the leader directs the support cell to dig the hole for the IED. Once dug, the leader directs another cell, to recover the IED from the cache, and emplace the device. Lastly, a triggerman,

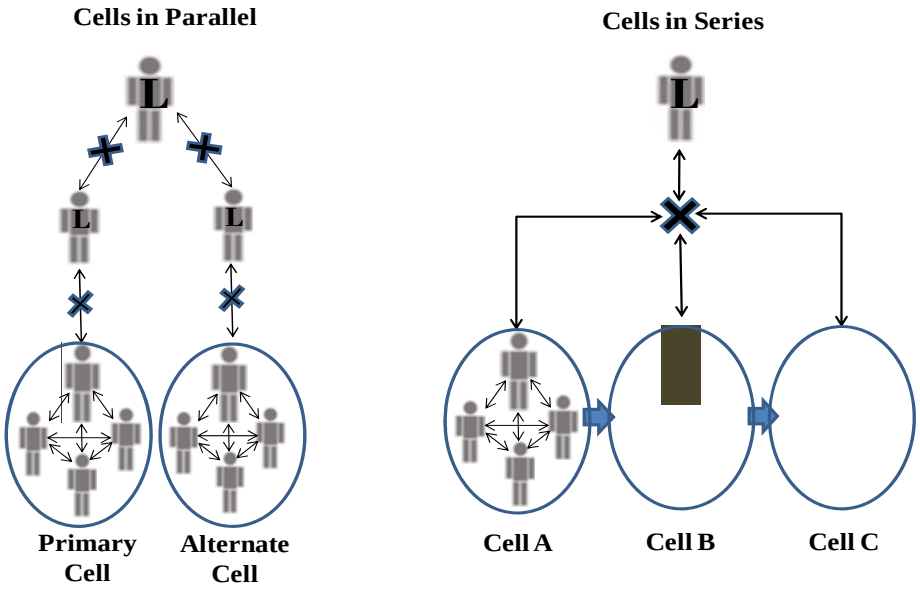

Figure 4. Examples of Cells-in-Parallel and Cells-in-Series[78]

Building upon the branch is the network, which is made up of multiple compartmentalized branches as shown in figure 2, generally following a pattern of intelligence (and counterintelligence) branches, operational branches (direct action or urban guerrilla cells), support branches (logistics and other operational enablers like propaganda support), and overt political branches or shadow governments.[79] Complex branches or networks, such as the example

---

from the operations cell, is provided with the means to detonate the device and the target description of the type of security force vehicle the IED was built to destroy, and conducts the operation. If he films the event, then he drops off the film at a drop-off point, and notifies the cell leader that the operation is complete. The cell leader directs the media cell to pick up the film from the drop-off site, and put it on the internet after editing it. See Grant, 6.

[78] Based on Figures 4-5, DA PAM 550-104, 25-26.

[79] Grant, 6.

network in figure 2, have a combination of cells and branches, and even individuals—especially leaders, in series and in parallel. The network has a leader that coordinates the efforts of his clandestine intelligence, logistical support, and operational cells, as well other elements, such as a local political wing or guerrilla force. He also has his own force-protection support, such as safe-house keepers, that operate the different locations he uses to hide during his daily routines. The leader may switch between his safe houses daily or every few hours to minimize the threat from counterinsurgents pinpointing his location.[80] The leader may have an evasion network that no one else in the organization knows about that he can use in an emergency. If he is the leader of a sub-network, also known as a branch, from a larger network, then he coordinates his efforts with his superior, who is responsible for a number of similar branches or sub-networks. This pattern continues to the core of the movement as shown in figure 2. These networks generally radiate out from the core members of the movement. They do not grow randomly or uncontrolled, nor do they follow strict mathematical growth—defined as self-organization—all of which can be found in different types of information-age networks.[81] Instead, they grow purposefully, either to link into supportive populations, to move into an area that the insurgents want to gain control of as

---

[80] Based on author's experience in Iraq. Insurgent leaders routinely moved between safe houses or safe locations based on the pressure from counterinsurgency forces, moving every few days to every few hours. Also see Bern, 110; Foot, 128.

[81] Albert-László Barabási, *Linked: How Everything is Connected to Everything Else and What It Means for Business, Science, and Everyday Life*, (New York, NY: Penguin Group, 2003), 16-17, 77-78; As As complexity theorists Simon Reay Atkinson and James Moffat explain: "Random Networks form through individuals meeting up by accident rather than by design;"and Simon Reay Atkinson and James Moffat, *The Agile Organization: From Linear Networks to Complex Effects and Agility*, (Washington, D. C.: DoD Command and Control Research Program, July 2005), http://www.dodccrp.org/files/ Atkinson_Agile.pdf [accessed January 12, 2009]. 97; Atkinson and James explain further, that small-world networks are defined by a low path length, or the "number of intermediate acquaintances that link one person to the other." 46; And finally, they explain that scale-free network links are based not on randomness, but based on an observation of the "richness of connection," or the number of links a node has, which increases the "richness of connection" of the node, which in turn causes these rich nodes to be connected to by random nodes due to "preferential attachment;" 47.

part of their strategy, or to gather intelligence around a specific target. As they grow, the leadership of the network decentralizes tactical decisions, but maintains operational and strategic control.

Clandestine cellular networks are largely decentralized for execution at the tactical level, but maintain a traditional hierarchical form above the tactical level.[82] There is an ongoing debate as to whether clandestine cellular networks are "networks" as understood today, or hierarchies.[83] Some experts believe they are flat organizations with near-real time interaction across the entire organization, others believe they are "leaderless" as well, with all members being relatively equal.[84] This monograph proposes that insurgencies are inherently hierarchies, but decentralized hierarchies. The core leadership may be an individual, with numerous deputies, to preclude decapitation strikes, or the core leadership could be in the form of a centralized group of core individuals, which may act as a centralized committee made up of core members. The core could also be a type of coordinating committee of like-minded insurgent leaders who coordinate their efforts, actions, and effects for an overall goal, while still maintaining their own agendas.[85] Without centralized control, the organization would not be able to effectively develop a strategy

---

[82] Grant, 6.

[83] Barabási, 17-18; Yaneer Bar-Yam, *Making Things Work: Solving Complex Problems in a Complex World*, (Cambridge, MA: NESCI Knowledge Press, 2004), 98-99; Sageman, *Leaderless*, vii, 69, 144; Brafman and Beckstrom, 5. Brafman and Beckstrom explain, "This book is about what happens when there's no one in charge. It's about what happens when there's no hierarchy."

[84] Ibid.; However, even though many theorist consider al Qaeda to have "leaderless" affiliates, the al Qaeda Training Manual makes it clear that there is to be a leader even if there are only three members, "'When they assemble, it is necessary to [have] a leader. Allah's prophet – God bless and keep him – even said, 'If three [people] come together let them pick a leader.'" *The Al Qaeda Manual*, trans.by the Manchester (England) Metropolitan Police, (no other publication data). http://www.au.af.mil/au/ awc/ awcgate/terrorism/alqaida_manual/ manualpart1_1.pdf [Accessed November 24, 2008], BM-12.

[85] Jeffrey, 5, 8.

based on ends, ways, and means, since each individual would not be bound to the common vision, which a hierarchy provides.[86]

Decentralization at the tactical level is due to the difficulty of real-time command and control within a large clandestine cellular network. As a result of compartmentalization and low signature for survival, network leaders give maximum latitude for tactical decision-making by cell leaders to maintain tactical agility and freedom of action based on local conditions.[87] The network leaders accept the risk that the subordinates may make mistakes, but due to compartmentalization, the mistake will largely remain local. The element that made the mistake may pay for their error, by being killed or captured, but the rest of the network is secure. The key consideration with regards to risk versus maintaining influence is to expose only the periphery tactical elements to direct contact with the counterinsurgents. This allows local adaptability to counterinsurgent tactics, as well as agility to maintain pressure on the counterinsurgents. In addition, the network leadership can replace the members of the tactical cells relatively easily if they are killed or captured.

---

[86] See Simson L. Garfinkel, "Leaderless resistance today," *First Monday* 8, no. 3 (March 2003): under "An introduction to leaderless resistance," http://firstmonday.org/issues/issue8_3/garfinkel/index.html [accessed on January 8, 2009]. As Garfinkel highlights, "Leaderless Resistance…has been used by white supremacists, anti-abortion and environmental activists, and animal rights groups. I argue that, despite the problems inherent in Leaderless Resistance, this structure is well-suited to many ideologies. Furthermore, many problems inherent in classic Leaderless Resistance can be overcome through modern communications technology. *This is not to say that Leaderless Resistance is an effective strategy for achieving a movement's stated aims. To the contrary, the adoption of Leaderless Resistance by a movement should be regarded as an admission of failure.* [author's emphasis] In many ways, Leaderless Resistance is a last-ditch effort to keep a struggle alive in the face of an overwhelming opposition."

[87] As 550-104 notes, "There is a great deal of local autonomy with respect to specific actions which require adjustment to local conditions. Tactical decisions are usually made independently by lower-echelon leaders in decentralized commands….There are two factors that dictate this practice. The first is that the local units probably know the situation better than the central command, and the second is that the lower echelons are probably better prepared to makes decisions with respect to implementation and time." Also see Grant, 6; "Each network concentrates its operations in a small geographic area such as a neighborhood or village, allowing each to focus on a specific American unit." DA PAM 550-104, 26-27.

Compartmentalization in Clandestine Cellular networks

The key concept for organizational form is compartmentalization of the clandestine cellular network.[88] Compartmentalization means each element is isolated or separated from the others.[89] Compartmentalization separates not only the clandestine elements from each other, but more importantly perhaps, the clandestine elements from the overt elements.[90] The ultimate goal for the organization is that no counterinsurgency operation can threaten the overall survival of the organization; there is always a portion upon which to re-grow the movement if necessary. It is the focus on long-term survival, or the "winning by not losing," which truly defines why this organizational form is used. As Trinquier noted, "The security of a clandestine organization is assured by rigorous compartmentation [sic]."[91] Structural compartmentalization is in two forms. First, is the *cut-out*, which is a method of communicating indirectly, ensuring that the counterinsurgent is unable to directly link two individuals together.[92] Second, is through lack of knowledge—no personal information is known about other cell members, aliases are used, and organizational or operational information is provided to members on a need-to-know basis only.[93] The 1966 Department of the Army (DA) Pamphlet 550-104 refers to this second method as the

---

[88] DA PAM 550-104, 2, 20; Prikhodko, 18-19; and Bennett, *Espionage*, 69.

[89] As defined on Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/compartmentalization [accessed on February 16, 2009].

[90] DA PAM 550-104, 2.

[91] Trinquier, 39.

[92] Prikhodko, 18-19; DA PAM 550-104, 2, 20; and Bennett, *Espionage*, 69.

[93] DA PAM 550-104, 20; Al Qaeda, BM-52-BM 55; as Grant notes, "Keeping his hands clean, [the network leader] avoids direct involvement in attacks by assigning operations and their planning to his lieutenants." Grant, 6; Bymann quotes a senior al Qaeda leader stating, "'When four people know the details of an operation, it is dangerous; when two people know, it is good; when just one person knows, it is better.'" Byman,109; also, as the al Qaeda training manual explains, "Keeping Secrets and Concealing

"fail-safe principle."[94] The amount of compartmentalization, as mentioned above, depends largely on the threat environment in which the organization operates, including physical terrain, the human terrain—passive supporters or hostile to the movement, and the perceived threat from the security measures and operations of the counterinsurgency force. As shown in figure 2, compartmentalization also separates the overt elements, the guerrillas and the political wings, of the insurgency from the clandestine elements as a further fail-safe.

The key for compartmentalization is that if any person in the network is detained, they have little, or preferably no, direct knowledge of the other members of their cell or network (see figure 5).[95] In any cell where the members must interact directly, such as in an operational or support cell, the entire cell may be detained, but if the structural compartmentalization is sound, then the counterinsurgents will not be able to exploit the cell to target other cells, the leaders of the branch, the sub-network, or overall network (see figure 5 and 6).[96] Thus, the structural compartmentalization protects the rest of the network. If however, the network has poor structural compartmentalization, then the counterinsurgents will be able to interdict a greater number of individual network members, until the counterinsurgents run into a portion of the network that is

---

Information," it states, "[This secrecy should be used] even with the closest people, for deceiving the enemies is not easy…."Seek Allah's help in doing your affairs in secrecy." *Al Qaeda*, BM-16.

[94] DA PAM 550-104, 2, 20.

[95] Ottis provides a good example of effective compartmentalization from evasion line networks in WWII, "Each escape line worker was one small link in a very big chain….While the workers concentrated on doing their jobs to the best of their ability, they did so without knowledge of the results of their efforts…..[One escape line worker] still [in 2001] does not know the details surrounding his involvement with the escape lines [in WWII]. His father maintained communications with the escape organization, and [the worker] simply followed his father's directions, escorting the evaders when and where he was told." Ottis, 68.

[96] Barnes, 44; Barnes' article captures the risk of direct contact between cell members, as the entire cell in this story is captured based on the questioning of individual members, thus revealing the names of the other members of the cell, which eventually leads to their arrest.

sufficiently compartmentalized to stop further exploitation (see figure 6 and 7). If there is no or poor compartmentalization, or if members of one cell are in direct contact with members of other cells in the same branch, or even members of other networks, compartmentalization features of the cellular hierarchy are then catastrophically negated.[97] This results in a "cascading failure" and the disruption, neutralization, or destruction of multiple cells, branches, or even the entire network may ensue (see figures 6 and 7).[98] In addition to the structural weakness in compartmentalization between a clandestine and overt element of the movement, there are weaknesses when different networks from different insurgent groups work together (also shown in figure 5). In the case of different insurgent groups working together, there is always an increased risk, since the compartmentalization in one group may not be as good in another, allowing a counterinsurgent operation to exploit this weakness if discovered and thus penetrate one network through another.

There may also be issues with compartmentalization when external support networks, either nation-state or non-state actors, provide combat, direct, or indirect support to the

[97] DA PAM 550-104, 207-208; also see Ottis, 20; Ottis provides an example of inadvertently negating the compartmentalization between networks from World War II evasion line in Europe, where it was discovered by the allies that two different escape lines were using the same rendezvous points without either network knowing. The allies were able to contact the two networks to deconflict. However, had the location been compromised to German security forces do to clandestine failures of one network, the other would have likely been discovered as well.

[98] Cascading failure normally refer to "overload failures" of complex non-human networks, but is used here in the sense of a counterinsurgent using intelligence driven operations, to "roll-up" targets in quick succession. For more information on cascading failures of non-human networks, see Adilson E. Motter and Ying-Cheng Lai, "Cascade-based attacks on complex networks," *Physical Review* E 66, (December 20, 2002): 1-4, http://chaos1.la.asu.edu/~yclai/papers/PRE_02_ML_3.pdf [accessed March 4, 2002. Also see Ottis, 96; Ottis provides a perfect example of a cascading failure due to poor compartmentalization, where a captured network leader provided the Germans over one hundred names of evasion line members, leading to the arrest of most.

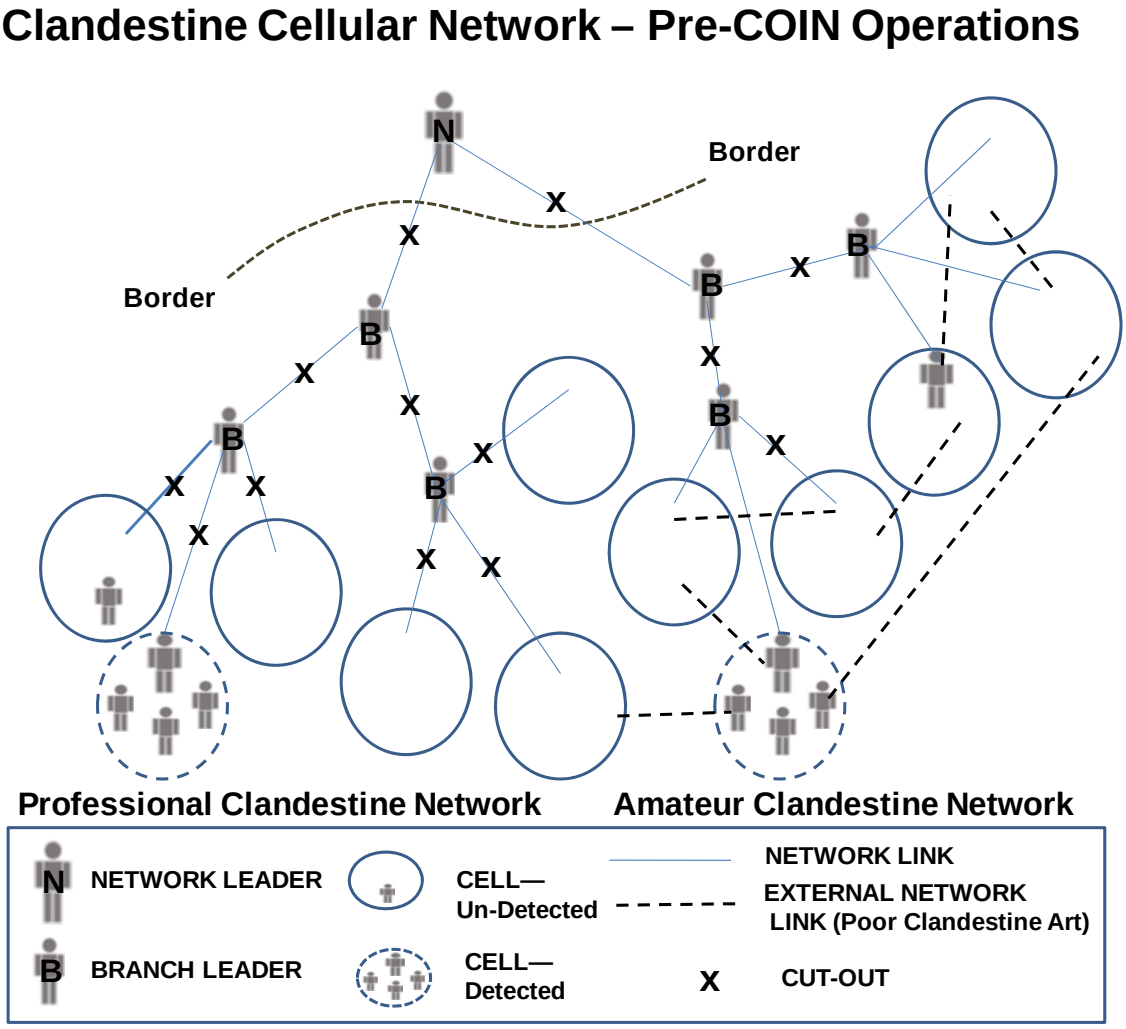

Figure 5. Examples of Compartmentalization—Pre-Counterinsurgency Operations[99]

insurgent network, also known as unconventional warfare.[100] If the two networks can build a solid relationship and the external support network is clandestinely sound, then the weakness is limited.

[99] Author's figure.

[100] This monograph uses the following definition of unconventional warfare: "operations by a state or non-state actor to support an insurgency aimed at the overthrow of a government [recognized or unrecognized by the international community, i.e. the Taliban] or an occupying power;" from D. Jones,

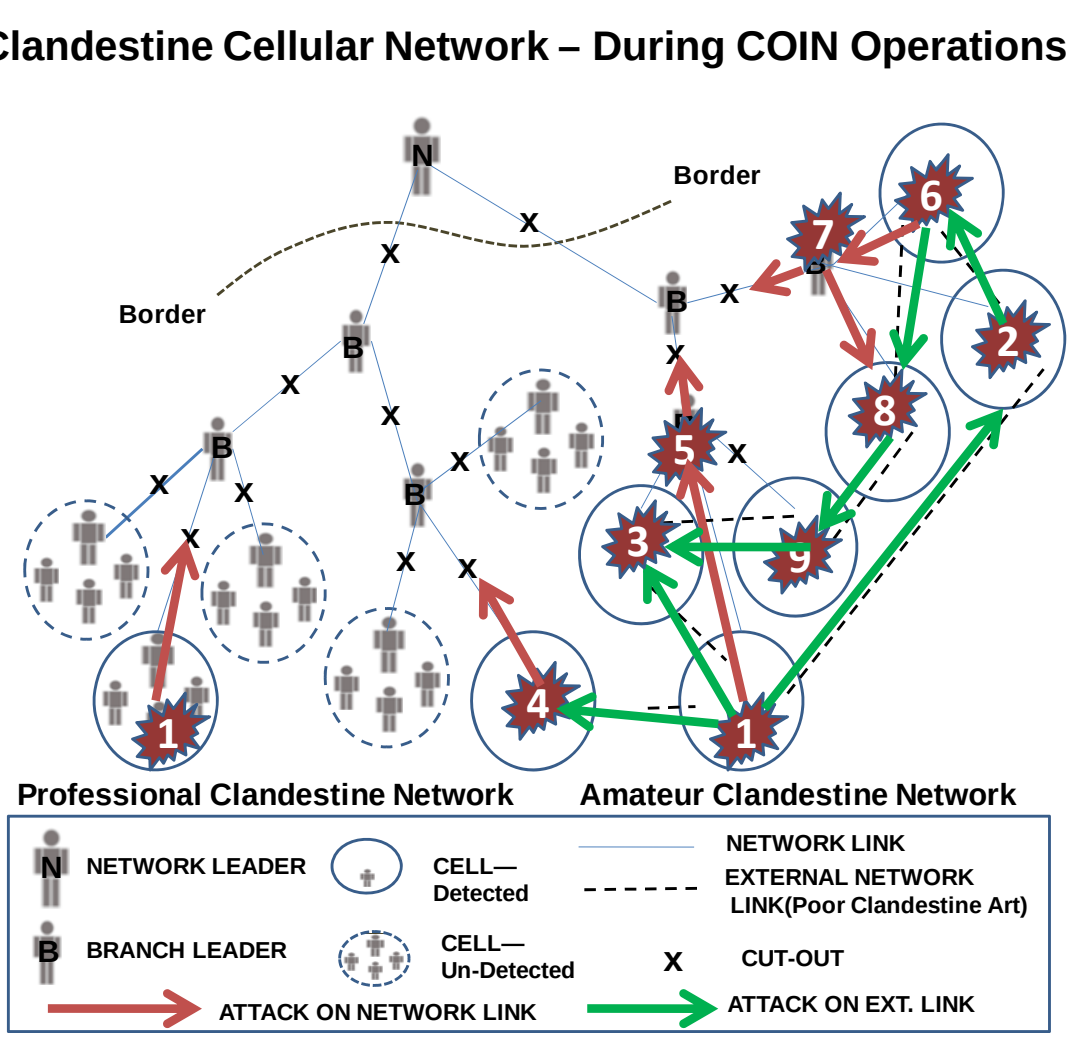

Figure 6. Examples of Compartmentalization During Counterinsurgency Operations[101]

Ending the Debate: Unconventional Warfare, Foreign Internal Defense, and Why Words Matter, (master's thesis, Fort Leavenworth, 2006), http://cgsc.cdmhost.com/cgi-bin/showfile.exe?CISOROOT=/p4013coll2&CISOPTR=554&filename=555.pdf [accessed on December 21, 2008], 165-166. For example, the al Qaeda Training Manual states, ""The main mission for which the Military Organization is responsible is: The overthrow of the godless regimes and their replacement with an Islamic regime." *Al Qaeda Manual*, BM-12.

[101] Author's figure. The figure portrays intelligence-driven operations against both professional and amateur clandestine cellular networks. Intelligence driven operations are frustrated when the counterinsurgents encounter the compartmentalization. Despite the significant success against the amateur network, the operations still fail to decisively disrupt or defeat the network. Without knowledge of the true size of the network, the counterinsurgents are unable to effectively assess success or failure.

The primary concern is with direct network-to-network interaction between a representative of the external supporter and one from the indigenous insurgency. For the nation state providing one of the types of external support—indirect, direct, or combat support—the representative could be an intelligence officer or members of a military special operations unit, interacting with their

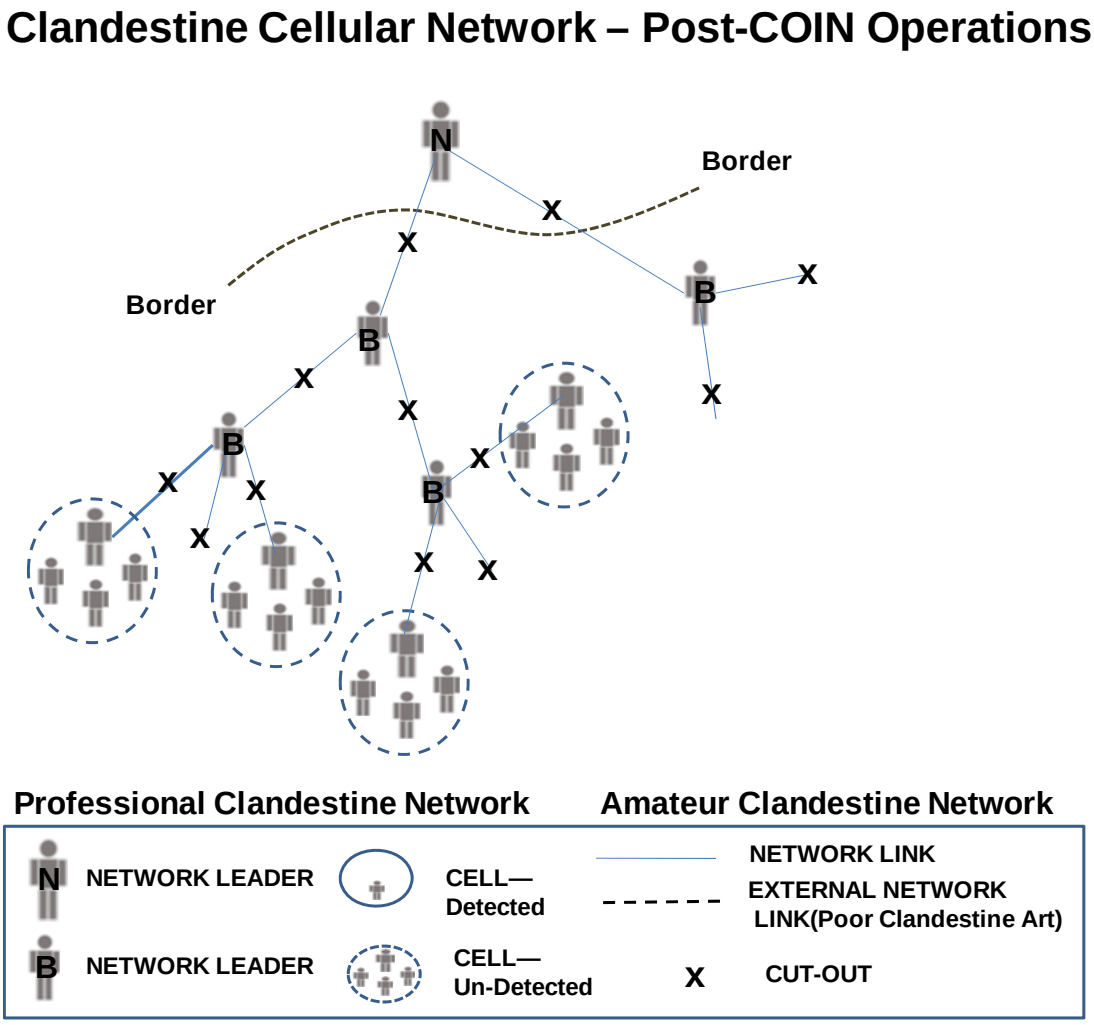

Figure 7. Examples of Compartmentalization - Post-Counterinsurgency Operations[102]

[102] Figure based on author's experience. Figure shows results of intelligence-driven operations against both professional and amateur clandestine cellular networks.

contacts in the insurgency within the country of conflict, in a sanctuary area, or in a third-party country, depending on a threat. This type of network interaction is not new. There are contemporary examples from Iraq, where Iranian nefarious activities have included the direct linkage from the insurgency to the Iranian Ministry of Intelligence and Security (MOIS) and Iranian Republican Guard Corps (IRGC) special operations forces.[103] Since 9/11, external support to insurgency has also fundamentally changed with the addition of a global non-state actor, al Qaeda, and its unconventional warfare efforts to support like-minded inter-state insurgent groups within the context of a larger global insurgency strategy. This type of support is best symbolized by Abu Musab Zarqawi's network in Iraq. Similar al Qaeda efforts can be found in other countries, such as Afghanistan, Pakistan, Indonesia, Algeria, Somalia, and the Philippines. In both state and non-state external support to insurgency, unconventional warfare is being conducted by the supporting state or non-state against the government fighting the insurgency.[104] Proper compartmentalization will largely protect all the organizations involved if employed correctly, or at least will forestall catastrophic cascading failures across the link between the external support network and the insurgency.

Understanding the Scale of Clandestine Cellular Networks

Lastly, it is important to understand "scale," or size, with regards to the organizational form of clandestine cellular networks. Although the basic building block is the cell, and in some cases may be a single individual, these elements are simply at the edge of a large web of

---

[103] See Jafarzadeh, 81-87; and Robinson, 107, 164,166-167, 342; White, 4; and Anthony H. Cordesman, *Iran's Revolutionary Guards, the Al Quds Force, and Other Intelligence and Paramilitary Forces*, (rough working draft, Washington, D.C.: Center for Strategic and International Studies, July 16, 2007), http://www.csis.org/media/csis/pubs/070816_cordesman_report.pdf [accessed on February 8, 2009].

[104] Jones, 165-166.

networks. A tree can be used as a visual metaphor for such a network, with branches and roots emanating from the trunk symbolizing the main network, the branches of the tree symbolizing the branches of a network, and the leaves representing the cells or individuals at the edge of the organization. There is an unwritten consensus that insurgent networks are generally less than a few dozen individuals, limited in scope, and localized, with little or no connection countrywide. However based on the Special Operations Research Office study in 1963, the size of the underground in historic interstate insurgencies have been surprisingly large: Palestine (1948)—30,000, Philippines (1946)—100,000, Greece (1946)—675,000, Malaya (1950)—90,000, Algeria (1956)—21,000, Yugoslavia (1940)—50,000, and France (1946)—300,000. [105] To understand how these underground elements get so large, the classic children's fable *The King's Chessboard* provides a practical model.[106] In this fable, the king offers to pay a wise man for his services, but the wise man, initially refusing payment, is forced to accept some type of compensation. The wise man asks to be paid in rice for each square on a chessboard, starting at one grain, and doubling at each square.[107] The king readily accepts the offer, failing to understand the exponential growth that will take place, much in the same way there is a general failure to understand the exponential growth of clandestine insurgent networks.

The amount of rice begins to grow from one grain of rice, to two, then four, then eight, then sixteen, and so on, until the number becomes so large it costs the king all of his rice.[108] The

---

[105] Molnar, et. al., 14-15.

[106] David Birch, *The King's Chessboard*, (New York, NY: Puffin Books, July 1993).

[107] Ibid.

[108] Birch. There are 64 squares on a chessboard and the exponential growth pattern is 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, 2097152, 4194304, 8388608, 16777216, 33554432, 67108864, 134217728, 268435456, 536870912, 1073741824, 2147483648, with the last number being to 32 squares from "The King's Chessboard

same thing happens within clandestine cellular networks, but is rarely understood. Each leader develops subordinate leaders who then become branch leaders as they develop their own subordinate leaders, and with this, the scale or potential size begins to emerge. Thus, the first piece of rice represents the initial core leader that at the second square branched into two subordinate leaders, who on the third square, each branch into two more, and so on. Each square represents new subordinate leaders and the last square represents subordinate leaders plus their cells. In just five squares, there would be sixteen cell leaders and their respective cells at the edge of the organization, fourteen branch leaders or sub-network leaders, and the original network leader. Imagining this metaphor applied in the context and scope of the historical examples of insurgency above, or against contemporary examples such as Iraq and Afghanistan, and the scale of the clandestine cellular networks begin to emerge.[109]

An open network, as described in the tree metaphors above, is growing purposefully, recruiting members to gain strength, access to targeted areas or support populations, or to replace losses.[110] Given proper compartmentalization, open networks provide extra security buffer for the

---

Solution," http://educ.queensu.ca/~fmc/march2003/KingsChessboardSoln.html [accessed on March 5, 2009].

[109] As one insurgent explained to author Zaki Chehab, "'We started this national front with ten people. We then opened it up to more people, and with the help of the faithful and those who believe in our cause, we have expanded to the extent that we have bases or cells all over Iraq.'" Zaki Chehab, Inside *the Resistance: The Iraqi Insurgency and the Future of the Middle East*, (New York, NY: Nation Books, 2005). Also, as Grant notes, "U.S. military officers described one such insurgent network, which calls itself the Islamic Patriotism Movement. Numbering about 55 fighters and led by a former Iraqi intelligence officer named Abu Omar, the network is loosely affiliated with the large Sunni insurgent group known as the Secret Islamic Army that operates throughout Iraq." Grant, 6.

[110] The author's open network construct is adapted from open and closed systems as described by the father of General Systems Theory, L. von Bertalanffy. Bertalanffy described a closed system, adapted in this case to networks, as "considered to be isolated from their environment." Using the same construct, an open network, based on the adaptation of system to network, is not isolated from their environment due to the requirement for purposeful growth; L. von Bertalanffy, *General Systems Theory*, 5th ed., (England: Penguin University Press, 1975), 38, 149, quoted in Shimon Naveh, *In Pursuit of Military Excellence: the Evolution of Operational Theory*, (Portland, OR: Frank Cass Publishers, 2000), 5.

core movement leaders by adding layers to the organization between the core and the periphery cells that generally have higher signature, and are interdicted more readily by the counterinsurgent. Using a tree as a metaphor, one can further visualize the relative security or clandestine capability based on the thickness of the portion of the tree: the trunk being the thickest, strongest portion, while the tips of the branches and leaves are the thinnest and weakest part of the tree. Yet regardless of where the tree is cut, even at its thickest point, if it still has roots, and given enough time, new saplings will emerge, and the tree will re-grow. This same idea applies to networks. Although the interdictions may disrupt operations in the short term, it causes the counterinsurgents to waste resources, time, and gives them a false sense of accomplishment, allowing the core to remain hidden and focused on long-term goals and strategies. While open networks are focused on purposeful growth, the opposite is true of the closed networks that are purposefully compartmentalized to a certain size, based on their operational purpose. This is especially pertinent to so-called "terrorist cells," a generally closed, non-growing network of specially selected or close-knit individuals.

Closed networks have a set membership, that generally does not change, and is indicative of cells, or special-purpose network, such as the members of the network involved in 9/11. Closed networks have an advantage in operational security since the membership is fixed, and consists of trusted individuals. The compartmentalization of a closed network protects the network from infiltration by the counterinsurgents. However, at the same time, as is indicative of some of the recent plots to re-attack the US or its allies, if there is a breach in security, the entire closed network generally is exposed and defeated. Once again, using the tree metaphor, the fruit of the tree would be characteristic of a closed network. Once it has fallen away from the tree to complete its purpose, it is its own self-contained entity that either completes its mission or, if the skin of the fruit is breached prior to the purpose being carried out, will rot, and the seeds will die. Since 9/11, much of the discussion on clandestine adversaries focuses on so-called "terrorist cells," failing to differentiate between open and closed networks, such as al Qaeda as a global

insurgency—an open network, and the 9/11 hijackers—a closed network—popularly described as a "terrorist cell or network." Noted theorist, Valdis Krebs mapped the 9/11 network, including the nineteen hijackers and numerous individuals that provided logistics support for the operation, yet never understood that this was a closed network.[111] Krebs' study has been used by numerous theorists to develop attack methodologies for use against so-called terrorist networks and insurgent networks, failing to realize that the closed networks and open networks have different forms, function, and logic, and thus require different applications of counternetwork theories.[112] Both examples highlight the fundamental difference between open and closed clandestine cellular networks, respectively. To understand the relative scale, it is also imperative to identify whether a network is open or closed.

There has also been a failure to appreciate the operational reach of open networks. Today, in Iraq it is estimated that over 80,000 insurgents have been killed or captured, likely a mix of overt and clandestine members of the organization, but regardless, it shows the magnitude that these networks can reach.[113] At the same time, experts fail to correlate any linkage between different elements of an insurgency or even linkage between disparate groups. For example, in 2005, RAND's Bruce Hoffman published an analysis of the insurgency in Iraq, concluding that the insurgency was a cluster of uncoordinated and disconnected local insurgent groups with no

---

[111] See Krebs.

[112] For example, see Barabási, 222-224; Borgatti, 1; and Matthew J. Dombroski and Kathleen Carley, "NETEST: Estimating a Terrorist Network's Structure," (lecture, Carnegie Mellon University Center for Computational Analysis of Social and Organizational Systems (CASOS), June 21, 2002), http://www.casos.cs.cmu.edu/publications/ papers/CASOSConf_2002_Day1.pdf [accessed November 22, 2008],13-16.

[113] David C. Gompert, "U.S. Should Take Advantage of Improved Security in Iraq to Withdraw" *San Francisco Chronicle* (December 2, 2007). http://www.rand.org/commentary/2007/12/02/SFC.html [accessed on November 10, 2008].

centralized leadership.[114] As he explains, "The problem in Iraq is that there appears to be no such static wiring diagram or organizational structure to identify, unravel, and systematically dismantle."[115] However, in hindsight it is obvious that the assumption of a disconnected insurgency was incorrect, and instead the linkages between the distributed cells were clandestine cellular networks and not readily visible to the counterinsurgent effort.[116] The visible parts of the networks were only the cells that were in direct contact with the counterinsurgent forces, at the periphery or edge of the organization, which practiced poor tradecraft and were detected and interdicted as shown in figure 8. Units that conducted operations against these cells had success

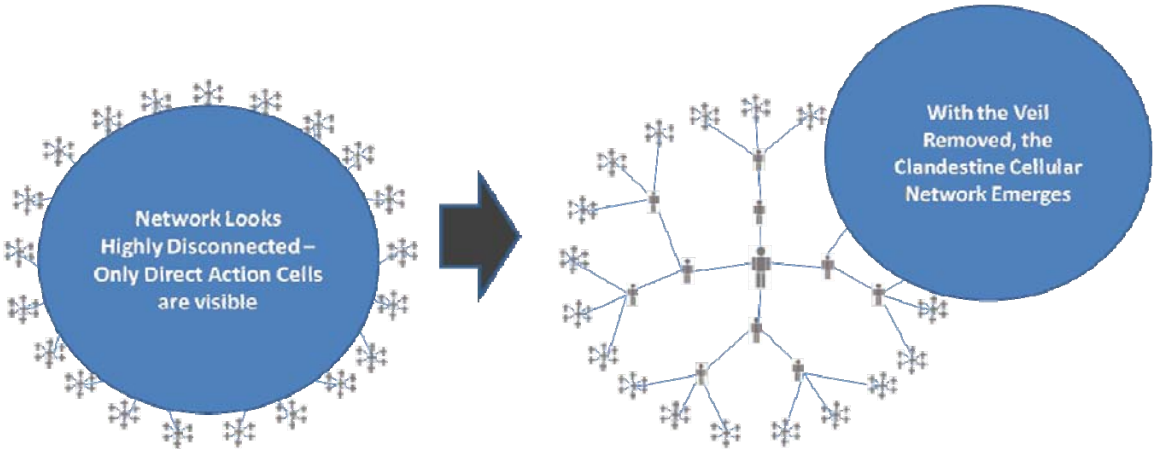

Figure 8. The Emergence of the Clandestine Cellular Network[117]

until they hit a compartmentalization mechanism, or cut-out, that stopped the exploitation, thus marking the boundary or edge of the clandestine organization (see figures 6 and 7).[118]

---

[114] Hoffman, *Insurgency*, 17-18.

[115] Ibid.

[116] White, 4-5; author's experience with members of the "Sons of Iraq," April 2007- November 2007.

[117] Author's diagram.

[118] For example, see Barnes, 44. Barnes captures the effectiveness of cut-outs and compartmentalization when the captured cell leader explains during questioning, "'Someone met me in

Interestingly, where one cell or network was effectively interdicted, in a short period of time, a new cell or network appeared.[119] As one former battalion commander commented to the author in 2006, "My battalion would [kill or capture] a cell and a new one will take its place within a couple of weeks at the most."[120] In hindsight, it is obvious, that the insurgency was connected and coordinated, behind the curtain of the clandestine space. [121] Although much of this hidden network relied on structural form to protect the network from pursuit by the counterinsurgents, the function of clandestine arts or tradecraft kept the signature so low that even experts like Hoffman did not realize the magnitude of the insurgency and its internal coordination.

All of these elements of organization form—from the component use of clandestine cellular networks to the scale, to the organizational hierarchy, have important meaning in the overall context or logic of this organizational form. Clandestine art or tradecraft—the organizational function—is applied to further protect this cellular or compartmentalized form.

Function of Clandestine Cellular Networks

Clandestine elements of an insurgency use form—organization and structure—to compartmentalize and minimize damage due to interdiction by counterinsurgents by limiting information distribution and interface with other members of the organization. Clandestine networks use function—clandestine art or tradecraft—to minimize signature and thus detection

---

Halibeah and gave me the [improvised explosive devices]'….He professes not to know names;" also see Robinson, 180. As Robinson highlights, "Doing so required a tip on one suspect's current location to permit 'time-sensitive targeting,' and his capture would lead to the next, and the next. On one single night, twenty-seven Al-Qaeda targets were successfully captured."

[119] Robinson, 180. As Robinson explains, "The Al-Qaeda in Iraq (AQI) organization had proven its ability to regenerate almost as fast as the commandos captured or killed its leaders."

[120] Non-attribution discussion with a former infantry battalion commander on his unit's operations against cells in Iraq, February 2006, Ft. Leavenworth, Kansas.

[121] Jeffrey, 1, 4-5, 8.

by counterinsurgent forces, and facilitate the communication between compartmented elements; in essence, functional compartmentalization, in addition to compartmentalization through organizational *form*, as explained above. Function is defined as "an action or use for which something is suited or designed."[122] It is the function of clandestine art or tradecraft to keep the network signature low so that the daily actions of the network remain undetectable by the counterinsurgent force.[123] These functions in clandestine cellular networks revolve around minimizing signature and detection of the interaction of members of the network and their operational acts. Clandestine techniques or tradecraft are used for the following: to conduct indirect or impersonal communications in order to *functionally* compartmentalize the organization; to minimize the signature of person-to-person communications, or "personal communications;" to conduct counter-surveillance; to reconnect the network when key leaders are detained or killed; to clandestinely recruit new members in order to purposefully grow the organization or replace losses; to hide key individuals using safe houses; to provide security for locations, such as meeting places and safe-houses; and lastly, to facilitate clandestine skill training between the superior and subordinates.[124]

Impersonal Communications

Impersonal communications, also known as cut-outs, functionally compartmentalize the networks as an additional precaution to the organizational forms of compartmentalization

---

[122] As defined on MSN Encarta Online Dictionary, http://encarta.msn.com/dictionary_1861613874/function.html [accessed on February 25, 2009].

[123] DA PAM 550-104, 6.

[124] See personal and impersonal communications, Prikhodko, 4, 19.

explained previously.[125] Impersonal communications, as the name implies, is anything other than face-to-face contact between two members of the organization.[126] Impersonal contact includes passive and active methods, the difference being in the type of signature produced.[127] Passive methods include mail- or dead-drops, live drops, and clandestine codes or signals hidden within different types of media.[128] Active methods include short or long-range radios, phone, and internet, all which emit signals that can be more readily detected by technologically capable counterinsurgents.[129] Impersonal communications is a method of ensuring that two individuals never come in direct contact, and thus cannot be physically linked to one another.[130]

Passive measures are used to minimize signature in extremely high-threat environments. Couriers are the most secure means of transmitting messages or moving items, such as weapons, between two individuals.[131] The key requirement for couriers are their ability to move some distance, including through counterinsurgent population-control measures, such as checkpoints,

---

[125] Prikhodko, 19.

[126] Ibid.

[127] Active and passive measures are the author's construct.

[128] Prikhodko, 19; and DA PAM 550-104, 20, 104.

[129] David Tucker and Christopher J. Lamb, *United States Special Operations Forces*, (New York, NY: Columbia University Press, 2007), 208-209.

[130] DA PAM 550-104, 102.

[131] DA PAM 550-104, 103; Orlov, 148-150; and Prikhodko, 18. Prikhodko places couriers within the category of personal communications, yet refers to couriers as a cutout, explaining "A 'cut-out' is an agent or subordinate officer used as an intermediary between the officer and the agent, to make surveillance more difficult." The author chose to keep courier as a method of impersonal communications due to the lack of interaction between the leader and subordinate. Also see Jones and Libicki, 129; Jones and Libicki highlight that, "[al Qa'ida] adopted a four-tiered courier system to communicate among key members of the group and *minimize detectability* [emphasis added]. Many al Qa'ida leaders have become more cautious in using cell phones, satellite phones, email, and other forms of communication that foreign intelligence services can easily track."

without arousing suspicion.[132] Women and children may be used as couriers to decrease suspicion and the chance of search if moving sensitive items or written information.[133] Although couriers are one of the most secure methods, they and their messages can be intercepted, as was the case with the letter sent from al Qaeda's Ayman al-Zawahiri to Abu Musab Zarqawi that exposed a rift between the al Qaeda core leadership and Zarqawi over Zarqawi's tactics against the Shi'a in Iraq.[134]

The second method of impersonal communication is the mail drop, also known as a letter drop or dead drop.[135] In this method, one member of the network places a message or item at a certain location, the drop site, which for larger items could be a cache. The deliverer then alerts the receiver, through other clandestine means, to pick up the item, resulting in no personal contact between individuals.[136] French counterinsurgency practitioner Roger Trinquier provides a description of the Algerian underground use of mail drops: "Carefully kept apart from other elements of the organization, the network was broken down into a number of quite distinct and compartmented branches, in communication only with the network chief through a system of letter boxes."[137] Although mail or letter drop describes the idea of leaving a letter or package in the Western mindset, and at times may include literally using the post office, this wording also

---

[132] Ottis, 78-79.

[133] Bern, 115; Orlov, 148-150; and DA PAM 550-104, 59.

[134] For translation of the letter, see Jumada al-Thani, trans., "Letter from al-Zawahiri to al-Zarqawi," *GlobalSecurity.org*, (July 9, 2005), http://www.globalsecurity.org/security/library/report/2005/zawahiri-zarqawi-letter_9jul2005.htm [accessed January 19, 2009].

[135] Trinquier, 13; Prikhodko, 20-21; Orlov, 150-151; Miller, 15; and DA PAM 550-104, 20-22, 33, 60.

[136] Orlov, 152; and DA PAM 550-104, 20-22, 33.

[137] Trinquier, 13.

symbolized that some unconventional locations may act as "mail boxes." Orlov provides some examples of the use of unconventional hiding places:

> Hiding places, such as a hollow in a tree…or a deep crack in a wall…or a hole bored in a public monument, take the place of mailing addresses….A special system of 'indicators' is used to orient each agent as to the specific hiding place where a message is awaiting him….The 'indicator' consists of a number or a symbol written on a wall, a park bench, or somewhere inside a railway station, post office, or public telephone booth."[138]

Thus the "item" is dropped off by one individual and then hours or days later, when the other individual sees the "indicator," he can recover the item, place an "indicator" signaling that he has retrieved the item, and thus ensures that both parties know the status of the communication while maintaining the anonymity.[139]

The third method of passive communication is the so-called "live drop."[140] The difference between a dead drop and live drop is that there is a person at the drop site that secures the item being passed between members.[141] This person is the cut-out, passing the item to the other member when they come to the location after being alerted that the item has been left with the live drop through some "indicator." As Prikhodko explains,

> When communicating by means of a live drop there is no personal contact….Operational materials from [deliverer]…are passed through a special person who more frequently than not is the proprietor of a small private business (book shops, antique dealers, [drug stores], etc.). The [receiver] visits the live drop…only after a special signal. The proprietor of the live drop places the signal after receiving the items.[142]

---

[138] Orlov, 152-153.

[139] Ibid., 153.

[140] Prikhodko, 19; and Miller, 71.

[141] DA PAM 550-104, 20-22, 104.

[142] Ibid.

The danger of this method is that if the individual that is the live drop is discovered, he has a direct link to the other member and may provide information that can lead to the interdiction of the other member.

Clandestine codes are the fourth method and can be used across different types of media to alert other cell members or pass information passively.[143] In print media, this could include ads or announcements in newspapers in which the information in the ad is a code that the other cell members understand.[144] In World War II, the Allies extensively used the nightly British Broadcast Corporation (BBC) overseas radio broadcasts to the resistance forces in Europe to pass information clandestinely on resupply drops and operational directives. These included the messages that only had meaning for the intended receiver, based on a code word intermingled in the broadcast, such as a forewarning of an impending parachute resupply drop to the resistance on a certain drop zone.[145] This same theory causes intelligence agencies to conduct in-depth of analysis of broadcasts by al Qaeda core leadership, primarily Osama bin Laden and Ayman al-Zawahiri, to see if there are any hidden messages.[146] Finally, code words can be innocuously inserted into emails or telephone conversations that for example could provide warning of

---

[143] Prikhodko, 23; and DA PAM 550-104, 231. 550-104 refers to this method as the "double-language technique" in which a form of media is used, but "contain messages and instructions coded in key words and phrases."

[144] Prikhodko, 25-27.

[145] Foot, 99.

[146] SPOOK86 explains, "You may recall that some of Al Qaida's earliest tapes depicted bin Laden and his deputy in outdoor settings (the nature hike, as some intel wags called it). The pastoral scenes ended when it was revealed that the CIA had hired geologists familiar with the rock formations of Afghanistan and Pakistan. Examining the rocks provided potential clues to the whereabouts of bin Laden and Zawahiri. More recent videos showed Zawahiri in front of a cloth or canvas backdrop. But even that "neutral" backdrop can reveal information that may lead analysts to a particular region where that material is commonly used." SPOOK86 [pseud.], "The Tape Zawahiri Had to Release," *In From the Cold,* formerspook.blogspot, entry posted January 31, 2006, http://formerspook.blogspot.com/2006/01/tape-zawahiri-had-to-release.html [accessed on January 24, 2009].

security forces approaching or execution orders to conduct operations against pre-approved targets.[147] Regardless of the means, it is the passage of information while maintaining a low signature that makes these very difficult to counter.

Active methods of impersonal communications—short and long-range radio, internet, landline, and cell phone—provide a much faster means of communications that has to be weighed against the increased risk of detection and interdiction by technologically sophisticated counterinsurgents.[148] Short and long-range radio transmissions have largely been replaced by phone. However, radios may be the only method of rapid communication in areas where there is no phone coverage. Radios may also be required if the instant passage of messages is required, such as an early warning alert of counterinsurgency forces moving into the area. Telephones, both landline and cell, have a role in impersonal communication, with the disadvantage of producing a signal which a security force could monitor. Phones can also be combined with passive measures, such as code words.[149] The internet has opened a new clandestine playing field, but like other active measures, there are still dangers due to an electronic signal. Thus instead of being a revolutionary adaptation, like the information age network theorists posit, the internet has opened a new clandestine playing field. The same clandestine techniques presented here have also been adapted to the cyberspace, including using cyber dead drops.[150] However, like other active measures, there are dangers due to the electronic signatures that can be detected by the counterinsurgents.[151] For example, Jihadists have also attempted to clandestinely hide their

---

[147] Grant, 6.

[148] Tucker and Lamb, 208-209; Byman, 96, 110; and Sageman, *Understanding*, 158-167.

[149] Grant, 6.

[150] See Wingate, 2; and Byman, 90.

[151] Byman, 85, 107.

webpage by piggybacking on other non-nefarious websites, often without the webmaster's knowledge, but they have been discovered in some cases.[152] Despite the strengths of active methods, such as rapid communications and long-distance reach, they significantly increase the danger for the insurgent due to the signals emitted that may be detectable by a technologically advanced adversary.[153]

Personal Communications

Meetings between members of a cell or network, who would normally be separated by one of the methods of compartmentalization, greatly increase the vulnerability of the two members.[154] However, despite the risks, there may be times when a clandestine leader needs to meet in person with his subordinates, instead of using an impersonal means, to gain better situational awareness, train the subordinate, assess the subordinate, or when the clandestine recruiting process, explained below, requires personal communications with potential recruits.[155] As I. E. Prikhodko explains from the perspective of an intelligence officer working with his subordinate agent, "

> Only by personal contact can the case officer study the agent better, analyse [sic] his motives, check on and control his activities, and finally---and this is of great importance—instruct the agent, train him in new methods and in professional [clandestine] skills, develop him, and exert an influence on him through personal example.[156]

---

[152] See Di Justo.

[153] As the al Qaeda training manual states, "It is well known that in undercover operations, communication is the mainstay of the movement for rapid accomplishment. However, it is a double-edged sword: It can be to our advantage if we use it well and it can be a knife dug into our back if we do not consider and take the necessary security measures." *Al Qaeda Manual*, BM-85 to BM-90.

[154] Prikhodko, 4.

[155] "Information and orders are passed during face-to-face meetings in mosques, where U.S. troops rarely go." Grant, 6.

[156] Prikhodko, 4.

Due to the vulnerability, meetings must be thoroughly planned including: identifying a meeting location, planning the routes of both individuals to and from the meeting location, establishing security to counter surveillance during the individuals' movements to the location, as well as having security around the location to give early warning and a plan if the meeting fails to take place.[157] As Swiss insurgency expert H. von Dach Bern notes, "meetings of [underground] members must be prepared at least as carefully as a raid, for they constitute a 'special type' of operation."[158] Specific types of personal communications and precautions are explained below.

Countersurveillance

Surveillance is the observation of a person or place to gain or confirm intelligence information, conducted by foot, vehicle, aerial, cyber, mechanical, and from a fixed location.[159] This section will describe the countersurveillance techniques practiced by the insurgent to defeat the counterinsurgent's attempts at surveillance.[160] Countersurveillance are the methods taken by the individual members for three purposes: one, to keep from being survielled while conducting insurgent-related activities; two, to determine if under surveillance; and three, to thwart active and passive surveillance in order not to expose other members, operations, or physical infrastructure of the network, such as safe houses or caches.[161] During the Cold War, surveillance

---

[157] Prikhodko, 4-13; Bern, 112-114; and Orlov, 110-125.

[158] Bern, 112; and DA PAM 550-104, 243-244.

[159] DA PAM 550-104, 243-244. Mechanical techniques include "wiretaps or concealed microphones."

[160] See *Al Qaeda Manual*, BM-85 to BM-90; this entire section is on how to conduct and defeat surveillance.

[161] Orlov, 110-125; and DA PAM 550-104, 104.

was a mix between stationary, foot, and vehicle surveillance.[162] These types of surveillance techniques can be used against cells and networks operating outside of zones of conflicts where the threat to the surveillance team is minimal. However, due to the difficulty of counterinsurgent elements safely conducting foot or vehicle surveillance in a high-threat counterinsurgency environment, today's insurgents have to contend more with aerial surveillance, both manned and unmanned, as well as other types of intelligence-collection platforms. During the hunt for Abu Musab Zarqawi in Iraq, an aerial-surveillance platform followed Zarqawi's spiritual advisor as he conducted a countersurveillance operation in which he quickly switched vehicles.[163] However, the aerial-surveillance package watched this countersurveillance maneuver and followed the spiritual advisor to where he met with Zarqawi, a fatal application of countersurveillance technique, leading to both of their deaths. Regardless of the types of surveillance employed by the counterinsurgents, low- or high-technology, the same basic countersurveillance principles apply.

The best method of countersurveillance is to keep from being detected in the first place. As DA Pamphlet 550-104 noted in 1966,

> A former underground leader has suggested that while it is difficult to completely escape modern surveillance methods, there are many ways to mislead the surviellants. The underground member, wishing to minimize risks and chance factors, attempts to be as inconspicuous as possible and refrains from activities which might bring attention or notoriety. He strives to make his activities conform with the normal behavior and everyday activities of the society in which he lives.[164]

---

[162] DA PAM 550-104, 243-244.

[163] Mark Bowden, "The Ploy," *The Atlantic* (May 2008): 4, http://www.theatlantic.com/doc/200705/tracking-zarqawi [accessed November 28, 2008]. As explained by a Abu Hayder, a detainee and a high-level associate of Zarqawi, "He explained that Rahman, a figure well-known to the Task Force, met regularly with Zarqawi. He said that whenever they met, Rahman observed a security ritual that involved changing cars a number of times. Only when he got into a small blue car, Abu Haydr said, would he be taken directly to Zarqawi.

[164] DA PAM 550-104, 101.

Having cover stories that provide a good reason for being in an area is one of the best methods of countering surveillance. For example, a clandestine network could use a delivery company driver as a courier, or could move large items, such as weapons, hiding them within the shipment, delivering the information and items as the driver makes rounds within an urban area.[165] Along the same lines, a larger shipping company may ship items to numerous locations within a country or even across borders, giving the clandestine network long-range operational reach to support larger networks spread out over geographic regions or even into sanctuary areas in neighboring countries. The possibilities are endless.[166]

Soviet clandestine operations expert I.E. Prikhodko refers to these measures as "counter-surveillance check routes which afford the most favourable [sic] opportunities for the detection of surveillance."[167] As Prikhodko explains, these check routes provide the clandestine operator a method of determining if they are under surveillance through a combination of traveling by different means (car, bus, train) and through different areas (urban, rural, congested, and sparsely populated) that would expose any surveillance package by forcing them to betray their activity.[168] If no surveillance is detected after a certain period of time using the check route, the clandestine operator can be reasonably sure that he is not being followed.[169] This technique is used by both

---

[165] Grant, 6.

[166] DA PAM 550-104, 103-107. 550-104 provides an example of countering inspection by security forces of hidden cargo, "An illegal cargo was covered with a tarpaulin and a layer of fresh manure. The police disliked searching such a load too closely and the cargo got through police inspection without being stopped;" 106.

[167] Prikhodko, 14; former Central Intelligence Agency case officer, Lindsay Moran refers to this exact same technique as a "'surveillance detection route." Moran, Lindsay. Blowing My Cover: My life as a CIA Spy. New York, NY: Penguin Group, 2005, 120.

[168] Prikhodko, 14.

[169] Ibid.

the leader and his subordinates if they are to meet, or conduct any other type of activity that may compromise other members or infrastructure if survielled. This technique could also be used to move to and from safe sites, caches, or dead drop locations. If surveillance is detected, then the clandestine operator cancels the meeting or other planned activities so as not to expose the other elements of the network or he attempts to lose the surveillance and continue the operation.[170]

Emergency Methods for Re-connecting the Network

Cellular or compartmentalized networks are by their nature resilient to attacks that kill or capture single individuals, to include key leaders, facilitators, or specially-skilled individuals, who have superiors and subordinates. These individuals will be referred to as nodes for clarity in this section. By compartmentalizing the organization, the damage done by counterinsurgent operations is minimized and allows for the re-connection of the network above and below the lost node. In this case, when a node is removed, emergency clandestine communications measures must have been pre-arranged by the leader prior to his death or capture, to ensure that his subordinate and superior can link up.[171] This prearranged method is developed in such a fashion that the instructions do not lead to the compromise of either party.[172] Thus, the reconnection procedure must be systematic and clandestine principles applied throughout. Without some type of secure and clandestine mechanism to reconnect the network, the network can be successfully fractured, and would be indicative of poor clandestine practice.[173] In some cases, a network can

---

[170] Orlov, 112-115, 156-157; and Clarence Ashley, *CIA Spy Master*, (Gretna, LA: Pelican Publishing Company, Inc., 2004), 231.

[171] Ottis, 92; Miller, 71-72; *Al Qaeda Manual*, BM-29 to BM-30; and Ashley, 132.

[172] Orlov, 112-115; and Miller, 71-72.

[173] Orlov, 113; and Ottis, 95.

reconnect if the members know each other well, but again, this ability is indicative of an insecure network that is operating more on luck than on any type of set clandestine procedures.[174]

In a well-structured clandestine cellular network, emergency communication methods are established throughout the organization from the higher level to the lower levels, as the organization grows, minimizing the threat of fracture.[175] The re-connection process can take place in four ways: 1) top down—the lost node's superior to subordinate; 2) bottom-up—subordinate to superior; 3) through a third party or intermediary, much like a live drop, providing a method for anyone in the organization to regain contact with the core network; and 4) through common knowledge of the other network members outside the individual's normal cellular chain of command, which happens in networks that are made up of individuals that know each other well.[176] Regardless of the method, the superior and subordinates may not know each other, and thus have to rely on pre-arranged recognition signals, codes, and specific actions when they meet.[177]

The first method is used when the higher level leader, the superior of the killed or captured node, makes contact with the subordinate through a pre-arranged method, such as a phone call and code word, or a visible signal, much like the one described by Orlov and used to mark a dead drop.[178] The superior establishes the special marking in a pre-designated location after the node has been removed. The subordinate knows that when he sees this emergency signal, he is to carry out a previously agreed upon action, given to him by his former leader, such

---

[174] Ottis, 94-95, 112-114.

[175] Molnar, et. al., 51; and *Al Qaeda Manual*, BM-30.

[176] Ottis, 92-98; Molnar, et. al., 80; and Miller, 71-72.

[177] Orlov, 152.

[178] Ibid., 151-153; *Al Qaeda Manual*, BM-29 to BM-30; and Ottis, 98.

as calling a certain number and using a code name, going to a certain location at a specific time to meet someone.[179] Once the two elements have linked up, the superior can provide the subordinate with further instructions on what to do and how to maintain contact. The superior may elect to promote the subordinate to replace the lost node, replace the lost node with someone else, or fill the role himself. Regardless of the method, a superior practicing good clandestine technique will immediately establish a new form of cut-out to protect the superior and subordinate once the meeting is complete.[180]

In the second method, the subordinate contacts the superior.[181] This method would be most likely used if the leader of the subordinate was captured, and the subordinate was worried that his leader may provide information leading to the subordinate's arrest. This may force the subordinate to flee, nullifying any attempt by the superior to use pre-arranged signals in the old area of operation. In this case, another set of pre-arranged emergency procedures would be used, where the subordinate established an emergency signal at a pre-designated location to alert the superior. As before, this would lead to the link up of the two elements, and the reconnection.

The third method, much like the live-drop described above, would be a location, such as a business, provided to all the members of a network, to go in case of lost contact.[182] A code word or code name would then be used to alert the owner or workers of the need for the individual to get in touch with a network leader.[183] Once the subordinate initiated the code word, he is given further instructions on how the superior would contact them to affect the link up. This method is

---

[179] Orlov, 112-113.

[180] Ibid.

[181] Ottis, 113-114.

[182] Prikhodko, 19.

[183] Ibid; Miller, 71-72.

risky for the location owner and workers since it acts as a funnel for multiple individuals to use to get in contact with network leaders. The individuals working at the location could be detained in an attempt to get them to provide information on the superior's location. This was the main method of the Allied evasion networks, where pilots were given a location to go to in order to get funneled into the network, but the Axis was able to infiltrate numerous agents acting as Allied pilots to fully expose these networks.[184] If the superior has established a solid cutout between the location and himself, then he, theoretically, is protected. The superior can further protect himself by controlling the meeting site with the subordinate, and establishing inner and outer security to observe if the subordinate is under surveillance.

In many cases, the superior and the subordinates do not know each other, which requires further clandestine methods during the actual physical link-up. It is the physical act of contact with an unknown subordinate that puts the superior at greatest risk.[185] He has to assume that the subordinate may have been detained, turned by the counterinsurgents, or perhaps provided them with the re-contact plan, and they have inserted an infiltrator, taking advantage of the lack of direct knowledge.[186] Due to this threat, the link-up is one of the most dangerous acts, and thus requires further application of clandestine methods.[187] It would be easy to meet at a pre-designated isolated location; however, this would make counterinsurgent surveillance easier if the subordinate was in fact working for them. Instead, the superior wants to blend in and use the human terrain to his advantage.

---

[184] Ibid., 3, 37-41, 81, 129.

[185] Orlov, 112; Also see Ottis, 114. Ottis provides an example of a failed meeting where minimal security measures were taken and resulted in the capture of the network leader.

[186] Ashley, 233.

[187] *Al Qaeda Manual*, BM-60 to BM-65

To do this he will establish a meeting location, likely in a very public place, such as a restaurant or market, with numerous escape routes.[188] The location would also provide an environment in which his inner and outer security elements could also blend into, or maybe even be part of the chosen environment, such as storeowners, sellers, and buyers in the market, or other jobs that are natural for the surroundings, in order to identify counterinsurgent surveillance. If the superior has indirect contact with the subordinate and can pass messages, he may provide detailed instructions, describing the exact route to take and will also provide a set of signals for recognition, emergency abort, and safe signals, as well as an alternate meeting plan if there is a reason the meeting cannot be carried out.[189] These instructions may also be passed through dead or live drops as well. If conducted correctly, the inner and outer security should be able to identify surveillance or determine if the subordinate is "clean." If they discover surveillance is following the subordinate, then the meeting is cancelled, and the superior escapes.[190] If not, then the superior and subordinate meet after exchanging recognition signals and code words to verify identities, and they can begin the process of reestablishing the network.

The final method happens in poorly compartmentalized networks and in networks built on pre-existing friendships, acquaintances, or groups, such as clans and tribes. In these cases, it is possible for individuals to re-link into the network through known individuals. This technique, with numerous links that bypass any cut-outs, such as members of one cell that interact with other cells, is indicative of a network with poor compartmentalization and clandestine practices, and could generally be categorized as an unsecure network, that is operating at a very high risk. Sherri

---

[188] Ibid., 119; and *Al Qaeda Manual*, BM-34.

[189] For examples of recognition and safe signals, see Prikhodko, 18; and Orlov, 112-114.

[190] Ibid., 115-116.

Greene Ottis' *Heroes: Downed Airmen and the French Underground* describes this method being used by some evasion line networks.[191] In some cases it works, mostly out of luck, but for the most part, it led to the destruction of multiple escape lines in World War II.

It should also be noted that regardless of the method of reconnection, once the link-up is successful, the superior will determine how best to re-establish the intermediate node. This will be done either through promoting the subordinate of the lost node, bringing in an outside individual that had not been previously part of the network, or simply by the superior taking over the role himself.[192] The course of action is likely determined prior to the meeting so that the superior only has to expose himself once during this emergency reconnection. If he can reestablish the cut-out simultaneously, then once the two depart, the network is generally safe again. If either individual is picked up leaving the site, they will not know the whereabouts of the other one. With the cut-out reestablished and the new reconnection instructions and clandestine communications instructions passed to the subordinate, the network can once again reconnect if one of the individuals is captured or killed by security forces soon after the face-to-face meeting.[193]

Lastly, with regard to elements at the edge of the organization, whose removal does not fit exactly into the category of requiring a network reconnection since there are at the end of a series of nodes or individuals, there still needs to be some consideration for the processes and implications of re-establishing the edge elements of the organization. The loss of an entire cell, or individuals (carrying out intelligence collection), generally marks the edge of the clandestine

---

[191] Ottis, 110-113, 133, 174.

[192] Byman, 17-18.

[193] Orlov, 112-115, 151-153.

organization. Due to their direct interaction, active or passive (in the case of an intelligence collector), with the counterinsurgent, they are innately at higher risk for interdiction than other network elements protected by at least one layer of cut-outs. However, the organizational form already accounts for this, understanding that these cells and individuals are easier to replace than say a core member or leader. Because they are naturally at the edge of the organization, there is little need for emergency reconnection, unless one of the cell members manages to evade capture, or later escapes from, or is released by, the counterinsurgents.[194]

In either case, they may attempt to regain contact with the network, which would then be done as explained above. These types of cells and individuals are the true "low-hanging fruit" of a clandestine cellular network and likely consist of individuals that are hired to carry out direct attacks or intelligence collection against the counterinsurgent force. In most cases, these cells consist of individuals that are formed by a cell leader who may or may not have training or experience in clandestine operations. Generally, the cell leader is the only individual that links to the main network through a cut-out, while the rest of the cell communicates amongst themselves. These individuals may simply be in need of money, desire to regain honor by fighting the counterinsurgent directly, or they are not competent enough for higher levels of responsibility in the organization.[195] They are hired to participate with the recognition by the network leadership that they will likely not last long against competent counterinsurgents. They will cause some

---

[194] Based on the author's observations in Iraq.

[195] Julian E. Barnes, "Cracking an Insurgent Cell," *U.S. News & World Report* (January 9, 2006), 44. Barnes report highlights the motivation of some insurgent recruits, "'I have six brothers…I have to support my family—that is why I did what I did.'" When the cell leader is captured, he explains why he took the leadership role, and in doing so shows how revenge drives many to insurgency and thus, care must be taken not to produce more insurgents than are killed or captured, "The reason I did this is that five from my family got killed by the Americans." As Chehab notes, "[the insurgent leader] replied that recruitment

disruption in their activities, but can be quickly replaced by other individuals with the same needs.

The core leader may determine that he can easily replace these edge elements should they get interdicted, and thus it is not worth spending time to teach anything other than rudimentary clandestine skills and the skills required for their specific mission. If the leader can replace a network simply by paying a group of individuals to attack the counterinsurgent force, and he can repeat this process indefinitely, than there is no incentive to waste time, and risk his exposure trying to link-up physically to train the group in clandestine arts.[196] This is especially pertinent when the cell is responsible for engaging the enemy, either directly with small-arms fire, or indirectly with an explosive device, and thus becomes a priority target of the counterinsurgent. This attention may serve another purpose, intentionally or not, but the counterinsurgent's focus on the kinetic elements of the insurgency, including these edge elements, gives the counterinsurgent something active to focus on, further protecting the clandestine elements. This is especially effective against western militaries that are focused primarily on the kinetic elements of the insurgency.[197]

This same idea holds true for more specialized cells that may have been employed directly by the core leadership as a special purpose cell, such as "terrorist cells." Although the special purpose cell is more difficult to replace because it is generally made up of trusted

---

was easy because people were upset by the inappropriate way American soldiers searched people's homes." Chehab, 21.

[196] "There were few jobs. For $50 or $100, groups could hire local Iraqis to take a shot at the Americans." Michael R. Gordon and Bernard E. Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq*, (New York, NY: Pantheon Books, 2006), 492.

[197] This illustrates the analogy that low hanging fruit may be nothing more than a security buffer between the more important cells.

individuals that are members of the core, it can still be replaced through internal reorganization or training personnel within the organization to perform the lost function. Regardless of the method of reconnection, once the link-up is successful, the superior will determine how best to re-establish the intermediate node, either through promoting the subordinate of the lost node, bringing in an outside individual that had not been previously part of the network, or simply by the superior taking over the role himself.[198] Regardless of the method of reconnecting the network, the loss of individuals requires not only the reconnection of the network, but a requirement to replace the lost node to deny any attrition affect on the network, either at the edge or within the core organization depending on which node was killed or captured. This process consists of a method of clandestine recruiting and can be used to replace lost nodes or grow the organization as needed.

Clandestine Recruiting

Although there is a perception that clandestine networks are largely made up of trusted and known friends and family members, reality throws this logic into a spin.[199] For an insurgency to be successful, it must increase in size and control.[200] While family and friends provide an added sense of security through loyalty bonds, and may well make up the members of the core group, few insurgent movements can be successful only having the support of their close friends

---

[198] Prikhodko, 33.

[199] For example, Sageman notes, "Evolution of the three main clusters [al Qaeda and its associated movements or the "Global Salafi Jihad," per Sageman] followed a pattern of growth through friendship, kinship, worship, and discipleship." Sageman, *Understanding*, 50; in this sense, the links outside friends and family when the movement begins are not the same as active recruiting that takes place at locations of religious "worship," and "discipleship" may be mistaken for part of the recruiting process, where the recruiter identifies, targets, befriends, and then disciples to a potential recruit prior to actually recruiting them.

[200] DA PAM 550-104, 7.

or family, including tribes and clans. They must branch out and increase their popular support in order to affect large political change. To do this, the organization must grow with purpose in order to gain access to the population, for resources, to replace losses, and to gain access to areas to target counterinsurgent forces. Thus, unlike information-age networks that grow randomly or without any control mechanism, such as the internet or social networks, clandestine networks grow with purpose—identifying low-risk individuals that bring skills, resources, intelligence, or access to targeted areas.[201] These individuals go through a process of clandestine recruiting.[202] Unlike the strong links between trusted individuals that have developed trust relationships prior to partaking in nefarious activities, clandestine recruiting is largely a method for recruiting unknown individuals or acquaintances of others, a form of social networking, and thus a weak link to the clandestine recruiter.[203] Generally, the recruiter is a network member that is purposefully gaining more links. The recruiter may or may not be a network leader, recruiting his subordinates directly. He could be a member of the core network who has the right kind of background or natural talent for recruiting, who recruits new members based on organizational needs, and then passes the

[201] As 550-104 explains, "underground recruitment techniques are probably most successful when selectively applied."DA PAM 550-104, 119; and Lindsay Moran, *Blowing My Cover: My life as a CIA Spy*, (New York, NY: Penguin Group, 2005), 33; also, *Al Qaeda Manual*, BM-15 to BM-16; under "Necessary Qualifications [for] the Organization's members."

[202] DA PAM 550-104, 111-119.

[203] Former Central Intelligence Agency case officer, Lindsay Moran, refers this process as the "recruiting cycle," consisting of the following steps, "spot, assess, develop, and recruit." Lindsay Moran, *Blowing My Cover: My life as a CIA Spy*, (New York, NY: Penguin Group, 2005), 33, 34; Sageman, *Understanding*, 122; Sageman refers to the same cycle; Buchanan 42-47. Buchanan uses weak links within social networking circles to show how weak links bridge strong link networks, this same idea applies to clandestine recruiting. In this case, the recruiter may have been given the name of a potential recruit or identified a potential recruit, then found an acquaintance of both the possible recruit and recruiter to introduce the two so as not to draw attention to the recruiter.

recruit off to a network leader for actual operational control.[204] This may in fact protect the network if the recruiting effort goes bad and a potential recruit turns in the recruiter. In this case, having good cut-out between the network and the recruiter protects the network.

The key for the clandestine recruiter is to never let on that he is recruiting for the insurgency until he has used his skills to identify, assess, and possibly test the candidate for recruitment, and that he is sure the recruit will accept his offer when finally approached.[205] The recruiter is looking for a recruit who has a personality for clandestine work, the right motivation, trustworthiness, loyalty, special skills or military background, access to a specific target location, population, intelligence, or resource of importance to the insurgency, and has the proper background—ideological, ethnic, or religious—to support the core movement's agenda. In some cases, if there is doubt about the recruit's willingness to work with the insurgency, the recruiter may have embarrassing background information to blackmail the recruit or he may simply gain

[204] See Sageman, *Understanding*, 142-143; for example, jihadi networks throughout the world have recruiters at local Mosques that can identify potential recruits, go through the recruitment process, and recruit these individuals if they are assessed to have leadership potential. Others with little long-term potential are provided instructions to get to the area of conflict and will be either foot soldiers, or martyred. For example, see Cordesman, *Iraq's Sunni Insurgents*, 2; *Al Qaeda Manual*, BM-93 to BM-98; provides detailed instructions on recruiting, including a recruiting cycle. An example of the type of individual that is good at clandestine recruiting is the "catalyst" from Brafman and Beckstrom, 120-129. Brafman and Beckstrom describe the "catalyst" as someone who are naturally inquisitive and interested in others, who like to meet new people, and all the while, are "mapping" them to determine their potential as members of the network. Brafman and Beckstrom's "catalyst" attributes all apply to the clandestine recruiter, despite their inherent business and social networking application in *The Starfish and the Spider*. Another possible location for identifying and approaching potential recruits is the counterinsurgent detention facilities. As Bob Woodward quotes a Defense Intelligence Agency report, "'Insurgent recruiters…exploit [detained individual's] feelings of humiliation, anger and fear to entice them to join the insurgency while in coalition custody or immediately after release;" Woodward, 35.

[205] DA PAM 550-104, 119.

compliance through coercion and threats to kill the recruit or members of the recruit's family if he does not cooperate.[206] If the person declines the offer to work with the insurgents, then the same methods of blackmail or coercion can be used to keep them from going to the counterinsurgents.

Another purposeful growth model, other than recruiting, includes insurgent leaders marrying into families, tribes, or clans, to gain instant rapport, loyalty, commitment, and access to the resources of the group, much like the monarchies of old, where the sons and daughters would be married to link kingdoms or countries.[207] This technique depends on the cultural and societal norms, but may effectively unite groups quickly. This is a favorite technique of al Qaeda to try to quickly gain the trust and backing of tribes, as was evident in al Anbar in the year leading up to the "Anbar Awakening."[208]

Safe Houses

Safe houses are used as part of core members' daily pattern of hiding from counterinsurgent forces, or if members are under pressure of pursuit by counterinsurgents and "need to go underground."[209] Safe houses are locations that should not draw attention, nor be readily connected to any pattern of insurgency or criminal activities.[210] These locations give the user a place to hide or stay, that has a built in, but invisible inner and outer security ring to

---

[206] Orlov, 93-95.

[207] Robert Windrem notes, "In some cases, al-Qaida security personnel have married into local tribes and clans, making them part of the extended family and giving Bin Laden and others additional protection." Robert Windrem, "Where is Osama Bin Laden? An analysis," *Deep Backgound: NBC News Investigates*, (June 13, 2008), under title, http://deepbackground.msnbc.msn.com/archive/2008/06/13/1138296.aspx [accessed on January 22, 2009].

[208] Author's experience in Iraq.

[209] Bern, 109-110; and Miller, 98.

[210] Ibid., 109-113.

provide early warning and protection.[211] Key leaders may use a series of safe houses daily to allow them to change location regularly to thwart attempts by counterinsurgency forces to interdict them. They generally move based on either early warning, or within the amount of time they believe it would take for the counterinsurgents to gather intelligence, develop a plan, get approval, and conduct the operation. This may cause them to move every few hours or days, depending on the perceived threats, the capability of their early warning, and how good an escape plan they have. It is not uncommon to hear of insurgent leaders who move every few hours each day to make sure that they are not captured.[212] If the counterinsurgents conduct operations against the safe house, but miss the insurgent leader, then the insurgent leader knows that he cannot re-use that safe house location without an increase in risk since the house may be under surveillance, or the informant that provided the information that drove the counterinsurgents to raid the location may still be active.

As shown in figure 2, safe houses are maintained by a subordinate leader as part of an operational support network.[213] The person that maintains the safe house is not involved in any other organizational functions so as not to draw attention and jeopardize the safe house.[214] The leader uses the safe house or safe location as randomly as possible so as not to provide the counterinsurgent with a distinguishable pattern amongst several safe houses.[215] At each location, a system of emergency signals would alert the user that the location is safe or not. For example, safe signals may be the "predesignated [sic] placement of shutters; flower pots; arrangement of

---

[211] Ibid., 112-113.

[212] Author's experience in Iraq and Kosovo.

[213] Bern, 110-111; and Ottis, 58-59.

[214] DA PAM 550-104, 223.

[215] Bern, 110-111.

curtains; open or closed windows; or clothes hanging on clothes lines."[216] Changes to these pre-designated signals would alert the leader that the site was not safe. The leader may also establish a personal evasion network or line, also depicted in figure 2, in which he establishes all the safe houses, safe-house keepers, and movement plans, himself, so that no one else in his organization knows.[217] This gives the network leader the ability to escape if the rest of his organization is detained. The evasion may be interstate, or extend over borders into sanctuary areas or other international locations.[218]

Security at a Location

Security at any location, such as meeting sites, safe houses, and dead drops, provide a means of early warning to give the network members an opportunity to escape or not approach the location.[219] To conduct this type of operation, the member responsible for establishing the location must have good communications with the members conducting security in order to get near real-time warning of impending danger. Two security rings are established—inner and outer.[220] Inner security is responsible with immediate security around the site, and may be armed to disrupt any counterinsurgent operations that penetrate the outer security without being detected in order to give the underground members time to escape. Outer security observes likely routes into the location that the counterinsurgents will use. A system for communicating must be

[216] Ibid., 110-111.

[217] Ibid., 111; and DA PAM 550-104, 222-226.

[218] Ottis, 41-43.

[219] Ibid., 113-114.

[220] DA PAM 550-104, 209; and *Al Qaeda Manual*, BM-57 to BM-58.

established, and may include cell or telephones, short-range radio, signals, or runners.[221] There should also be an agreement on actions of the security elements and the individuals at the location, whether to fight, flee, or if the security elements will fight the counterinsurgents to give the key network members a chance to escape.[222]

In some cases, the security elements may simply be passive, watching key counterinsurgency locations such as bases or airfields, or the elements may be individuals infiltrated onto one of these installations—such as cooks, maintenance personnel, laundry facility workers, contractors, or even interpreters— that provide a form of outer-ring early warning, but within the enemy camp.[223] This passive security measure could include overhearing conversations between soldiers about upcoming missions or information found in the trash. In the case of locally hired interpreters, they may even be directly briefed on upcoming missions against the network that they actually work for, thus providing the ultimate security and situational awareness for the network leaders. If the interpreter deems the threat to be immediate, then he can risk calling the network leader direct with the warning. In the case of infiltrators whose duty does not allow for daily movements on and off the counterinsurgent installation, such as the interpreter who may have ongoing operations or strange hours due to ongoing operations, or the information is not time sensitive, then another clandestine communication method can be used. For example, other local-hires purposefully infiltrated onto the installation by the network leaders with regular

[221] DA PAM 550-104, 209; an example from 550-104, used by the Huks in the Philippines, "If government troops approached a village and a man chopping wood observed them, he would increase the rate of his swing. A woman noticing his increased pace would place a white and blue dress side-by-side on the clothesline. Other members of the security net would pass the warning on that a government patrol was in the area."

[222] Bern, 113-114.

[223] Ibid., 127-139.

daily schedules may be the courier between the network leaders and interpreter or other intelligence gatherers. In this case, they may use a dead or live-drop procedure to pass the information, or the courier may use the same method to pass instructions from the leaders to the agent.

Other passive outer-ring security techniques may include recruiting business owners whose businesses sit astride likely counterinsurgent routes, or even outside the gates of counterinsurgent installations. The movie *Blackhawk Down* also provides an example of outer security, where a young boy is paid to sit and overwatch the airfield. He then phones the cell leader to report activity, in the case of the movie, the over flight of a large helicopter assault force departing the airfield.[224] Passive security can consist of anyone that does not draw attention of the counterinsurgents.

Clandestine Skills Training

New and old members must be continually trained and tested on the clandestine methods above to make sure they are not violating the clandestine procedures of the network.[225] As Prikhodko explains,

> Clandestinity in agent operations is directly dependent on the indoctrination...keeping in mind the main objective: to offer assistance, to show how to fulfil [sic] his assigned task better and more securely, [and] to help correct mistakes he has committed or eliminate inherent shortcomings.[226]

---

[224] Simon West, Mike Stenson, Chad Oman, and Branko Lustig, "Scene 5," *Black Hawk Down*, DVD, directed by Ridley Scott, (Culver City, CA: Columbia Pictures, 2002).

[225] Ney notes, "Personal security is of such primal necessity—that it must be continually and continuously checked and inspected by the resistance members. Even the slightest slip of security must be corrected drastically and on the spot by the members observing it." Ney, 155; and Prikhodko, 33.

[226] Prikhodko, 34.

However, the best training is risky due to the fact that the leader and subordinate must meet in person until the leader is confident that his subordinate is trained.[227] This training can take place in any secure location and may include any of the functional skills described above, as well as operational skills required by the individual, such as the employment of new weapons systems.[228] As Prikhodko notes, "The [network, branch, or cell leader's] task is to train [subordinates] properly and to transfer [them] to impersonal forms of communications in good time."[229]

If the insurgency is receiving external support and is directly working with intelligence or special operations personnel from the external supporter, personnel may undergo specialized training in tradecraft and other clandestine operational capabilities. During the Cold War, communist insurgent leaders received extensive training by communist regimes, especially the Soviets, such as the courses taught at the Lenin School.[230] The ability of nation states and non-state actors to provide this type of in-depth training continues today, but much more covertly, to provide plausible deniability, such as the training provided by Iran to Iraqi Shi'a insurgents.[231] This training may be conducted simply during a personal meeting between the underground member and the external support representative locally or could include training outside the country of conflict, such as in sanctuaries or other locations chosen by the external supporter. Person-to-person training, as noted above, increases the risk of all parties involved, but training at

---

[227] Lindsay Moran, *Blowing My Cover: My life as a CIA Spy*, (New York, NY: Penguin Group, 2005), 206-207.

[228] Skills may also be transferred under from one organization to another in counterinsurgent detention facilities. As author Bob Woodward directly quotes from a Defense Intelligence Agency report, "'Insurgents and terrorists use coalition detention facilities to trade information on successful tactics and techniques, teach detainees insurgent and terrorist skills, preach radical Islam and recruit new members into the insurgency;'" Woodward, 34.

[229] Prikhodko, 33.

[230] DA PAM 550-104, 121.

external sites provides the opportunity for intense training to be conducted while not under pressure of the counterinsurgents.

The last method is training conducted almost as independent study, including reading historic literature, manuals produced by the insurgent organization, or viewing on-line references. Obviously, this is the least preferred method for training individuals in the organization. The internet provides a balance, with the ability to provide video, and rapidly disseminate new tactics, techniques, and procedures, but still far from perfect. Without controlled or precision distribution to desired individuals, the counterinsurgent can view and learn from these as well. The medium for distribution may also not reach isolated individuals. STRATFOR's Fred Burton correctly identifies the problems with this type of training in tradecraft,

> While some basic [clandestine] skills and concepts…can be learned in a classroom or over the Internet, taking that information and applying it to a real-world situation, particularly in a hostile environment, can be exceedingly difficult. The application often requires subtle and complex skills that are difficult to master simply by reading about them: The behaviors of polished tradecraft are not intuitive and in fact frequently run counter to human nature. That is why intelligence and security professionals require in-depth training and many hours of practical experience in the field.[232]

Thus, freedom of movement is paramount for clandestine leaders to gain access to their network members, especially new members, and provide clandestine training if they expect their subordinates to survive.

This is one reason why prior to transitioning from the latent and incipient phase to other phases of an insurgency, the core group attempts to establish an extensive clandestine cellular network, to include training subordinates, before counterinsurgent operations and population control measures can be implemented. This requirement for personal contact for training provides

---

[231] Jafarzadeh, 108.

[232] Burton.

the counterinsurgent with an exploitable weakness of clandestine networks—the requirement for freedom of movement. Without freedom of movement, the result of population-control measures that isolate the population from the insurgents, the insurgent leaders are unable to replace, further develop, or grow a clandestinely competent network that has a chance for long-term survival. This explains why the periphery elements, or the low-hanging fruit, of the clandestine organization may receive little or no clandestine training, since these elements can be replaced more easily and with less risk to the network than it would take to train them to be proficient.[233]

Logic of Clandestine Cellular Networks

From an understanding of the form and function, the logic behind clandestine cellular networks emerges. The main purpose of this organizational form and the way it functions is for long-term survival in order for the movement to reach its political endstate. Every aspect of the form, function, and logic is focused on limiting damage from counterinsurgent strikes or making it difficult for the counterinsurgent to find something decisive to strike. It is about balancing the need to conduct operations to gain and maintain support while also protecting the core movement. It is these aspects of clandestine cellular networks that are difficult for western theorists and practitioners to understand and recognize because they generally do not have a worldview based on the idea of *long-term* or *survival*. The West has grown accustomed to quick conventional wars and has a difficult time understanding how any individual would be willing to live under the strain of a clandestine lifestyle, constantly in fear of being killed or captured, willing to risk everything for a cause, and operating this way for years or even decades. As DA PAM 550-104 explains:

---

[233] Gordon and Trainor, 492.

> To fully understand how and why an individual makes certain decisions or takes certain actions, it is essential to understand how he perceives the world around him…. [Individuals] assume roles which are defined by the nature of the organization. For this reason knowledge of underground organization is important and prerequisite to the understanding of the behavior of underground members. When an individual joins a subversive organization, the organization becomes a major part of his daily life and alters his patterns of behavior markedly.[234]

Clandestine cellular networks are also not easy to understand militarily since the whole premise seems conniving, unjust, and subversive, versus the accepted nobility of modern warriors, who practice overt lethal operations. It is the reason western militaries are drawn to fighting overt guerrillas, and why the current and past doctrinal publications focus so heavily on the counter guerrilla fight, yet barely mention anything about the underground.[235] Overt military units, with general hierarchal formations, are readily understood by western militaries; they do not understand clandestine cellular networks. It is the same reason that the modern ideas of "networks" do not seem to capture the form, function, and logic of insurgent networks either; and why in the absence of understanding, theorists and practitioners alike will apply their own understanding of networks based on western perceptions. Thus, they cognitively force the square peg of "clandestine cellular networks" into the round hole of modern "information-age networks." The logic of clandestine cellular networks is the antithesis to technologically focused conventional warfare and highly connected information-age networks. Based on this study, the reality of clandestine cellular networks and their form and function presents a very different picture. The final element is the systemic understanding of the logic based on the movement's survival in order to achieve its political goals.

---

[234] DA PAM 550-104, 15.

[235] See FM 3-24, 1-17, 1-19 to 1-20; *U.S. Government Counterinsurgency Guide*, (Washington, D.C.: Bureau of Political-Military Affairs, 2009), www.state.gov/t/pm/ppa/pmppt [accessed March 25, 2009], 26.

Goals and Survival

The overall political goals of the movement are the definite driving force behind the logic of the organization. The successful accomplishment of the goals is partly driven by the strategy, the ideology, or motivation, but ultimately rests on the fact that the organization must survive to reap the benefits of its struggle.[236] Successful accomplishment of the purpose of the insurgency, whether to coerce, disrupt, dissuade, or overthrow a government, or force the withdrawal of an occupying power, rests on its ability to maintain its potential for carrying on the conflict—winning by not losing—which is why the organizational form, function, and logic of clandestine cellular networks matter. It provides a means of keeping the core members alive, regardless of setbacks. The clandestine network will gladly sacrifice the overt elements for the sake of the clandestine element's survival.[237] It will revert to the latent and incipient phase if necessary and will wait for better conditions, which may be months, years, or decades.[238]

Time for the insurgent relates to the desire and motivation for accomplishing the goal, not convenience or impatience. This also separates those insurgents that can be morally and cognitively defeated, generally based on grievances or false motivating factors that prove unreachable, and those that will require killing or capturing, which are generally the

---

[236] "The object of war is specifically 'to preserve oneself and destroy the enemy;'" Mao Tse-Tung, *On the Protracted War*, (Peking, China: Foreign Languages Press, 1967), 61-63; 61; and McCuen, 51-52.

[237] McCuen explains, "more important from the revolutionary point of view is that a primary objective is preservation of the revolutionary forces. As long as these forces exist in some form, the governing power must conduct expensive and tiring operations." McCuen, 51.

[238] Sir Robert Thompson referred to this as "the famous 'one step backwards'" for insurgent movements, and noted, "When facing defeat, both militarily and politically…it [may] be considerably more than one step." Thompson, 43; also, "The element of duration makes a vast difference in the intrinsic structure of an underground movement. If for example, it is based on the assumption of a protracted war, then the entire plan and strategy must be radically different from one organized for a short term only;" Jan Karski, *The Story of a Secret State*, (Boston: Houghton, Mifflin Co., 1944), 231, as quoted in Ney, 46.

ideologically-motivated individuals, driven by religion, culture, or ethnicity. The core may apply other, less-overt means of conflict to create space and time to regenerate or strengthen the underground. These measures could include: 1) using overt political wings to attempt to reach the goals through non-violent means, while increasing the strength of overt and clandestine elements in the insurgency if non-violent means are unsuccessful; 2) ending lethal operations and going completely underground until more favorable conditions exist; 3) agreeing with government cease fires in order to rebuild the organization; and 4) reconciling with the government, but demobilizing only the overt elements of the movement. All of these measures are meant to ensure the key parts of the organization survives to fight the insurgency another day.

The combination of attaining goals and survival explains the logic that makes insurgencies so difficult to defeat, and why insurgents that use the protracted war theory, in conjunction with this logic, can wear down a government, an occupier, or a nation state providing external support to the host nation.[239] This is the same reason why insurgencies that use the military focused strategy (FOCO), or have a single charismatic leader, succeed only when the governments they face are incompetent. In these cases, if the government practices counterinsurgency with some competence, they can defeat these movements. Military-focused movements and movements built around a charismatic leader can be defeated because they lack a solid clandestine cellular network upon which to build the movement, while simultaneously providing the organization with resilience in the face of setbacks.[240] Conspiratorial insurgencies, on the other hand, are primarily underground, and thus can survive a long time, but may lack the

[239] FM 3-24, 1-6 to 1- 8.

[240] Ibid., 1-5.

mass—physical, moral, or cognitive—to pose a serious threat, unless it is capable of fomenting a mass uprising or conducting a coup d'état.[241]

Israeli military theorist Shimon Naveh provides an interesting and applicable interpretation of goals. He notes that military systems, which based on their use of violence, loosely describe insurgencies, having two "interaction characteristics." The first, matches with the organizational form of a hierarchy with decentralized execution as found in clandestine cellular networks, which Naveh refers to as the "succession of echelonment." This is based on "a deep setting, hierarchal structure and a columnar mode of relation between the system's components, or between sub-systems within the overall system."[242] Second, is "the absolute dominance of the system's [goal]," which as Naveh explains, "the initial assertion of the [goal] of the system's brain or directing authority predetermines the comprehensive whole, i.e. the all-embracing accomplishment of its future destined action."[243] In this sense, the use of a clandestine cellular network as the organizational form is inherent due to the insatiable desire for organizational survival in order to succeed in its political struggle. This same theory is behind the historic conspiratorial insurgency, and shows the amateurish idea of a military focus (FOCO) insurgency as espoused by Che Guevara, who may have survived the application of this theory in Cuba due to the ineptness of the Batista government, but paid with his life for using it in Bolivia.[244] Despite

---

[241] Ibid., 1-5.

[242] Naveh, 5.

[243] Ibid., 6.

[244] Henry Butterfield notes, "The Kremlin had long entertained misgivings about Havana's strident views of revolution, its determination that the job of revolutionaries was to make revolution and not wait for favorable conditions." Henry Butterfield Ryan, *The Fall of Che Guevara: A Story of Soldiers, Spies, and Diplomats*, (New York, NY: Oxford University Press, 1998), 61.

this desire to achieve its goals and survive, the cellular network members undergo extreme pressures and stresses.

Pressures and Stresses in Clandestine Cellular Networks

In order to understand the logic of clandestine cellular networks, it is imperative to understand the effects on the members of the organization due to the constant physical, moral, and cognitive pressures that clandestine members must live under. The simple fact that clandestine networks operate under the constant pressure of "death or capture," further delineates clandestine cellular networks from information-age networks.[245] Individuals involved in information-age networks, such as the internet, business, or social networking, do not normally operate under the pressure of being killed or captured.[246] They may have pressures such as market share or popularity, which may equate to "survival," but in response, these networks survive by having the largest signature as possible, to draw new clients, business contacts, or market share. The pressures on the clandestine individual differ most readily in the fact that members of the organization must practice clandestine arts in every aspect of their lives, or risk death or capture. Author Raymond Momboisse, in his book *Blueprint of Revolution*, provides an interesting summary of the pressure of clandestine life:

> Underground work itself, even if stripped of all danger, is hard work. It must be done meticulously and yet at high speed. But danger cannot be removed; it is an integral part of the way of life and it takes its toll physically and mentally. The pressure is beyond

---

[245] As Moran explains the pressures of working as a CIA case officer, "*I've been doing this spying thing for months now, and I've realized: You can never be one hundred percent sure [you are not being* surviellled]. *Still, my eyes are trained to dart around at all times, even when I am doing everyday errands or just out for a walk. I'm constantly on the lookout, and on a night like tonight, all my senses are on high alert. I feel less like a predator and prey. Truth be told, I am almost always terrified of getting caught*." Lindsay Moran, *Blowing My Cover: My life as a CIA Spy*, (New York, NY: Penguin Group, 2005), 186.

[246] As Orlov notes, "In the life of an underground operative nothing is as simple as it is in the lives of ordinary, carefree people." Orlov, 110; also see Foot, 163; and Sageman, *Understanding*, 132.

> description. The underground worker constantly lives on nerves, as he must, watching his every move, his every word. The work stretches nerves and fatigue stretches them even further, but it is the constant fear that nearly snaps those nerves. The agent cannot let anything go unnoted and unquestioned. He is in a constant state of fear, indeed, he must be, for it works to keep him alive. It maintains the instincts of self-preservation on continuous alert.[247]

When they fail to practice the clandestine arts or establish their networks in accordance with a secure organizational form, they begin to have an increased signature which the counterinsurgents can exploit.

The pressure also mounts as other individuals within the network are killed or captured, especially for the superior or subordinate of these individuals.[248] Depending on the experience level of the leaders and members, the removal of individual nodes within the network, or cells that are on the edge of the organization, may or may not cause an increase in pressure. Generally in an experienced network, with solid form and functional compartmentalization and practices, single nodes or periphery cells being killed or captured is expected, and well within the tolerance levels of the network. While disconcerting, it is not demoralizing. Thus, any successful counternetwork theory would have to push the clandestine leaders and members out of their comfort zone and cause them to make a decision that would ultimately lead them to increase their signature and expose themselves.

This would be a type of operation that was outside the tolerance of form, function, and logic of clandestine cellular networks. This type of pressure forces the clandestine cellular network members to be immediately proactive in their response in order to either protect

---

[247] Momboisse, 64.

[248] As Moran highlights her fear for her agents, "I was on the lookout all the time. *Am I being followed? Is someone following one of my agents? Is my phone tapped? Is my house bugged? Where would they have planted the video cameras? What if I get arrested? Worse yet, what if one of my agents gets*

themselves, their network, or attempt to regain situational awareness. Seasoned clandestine operators overcome some of this anxiety by trusting that the form and function that protect and reconnect the network is still sound. Experience and confidence increases for those individuals unfortunate enough to get detained and questioned, but eventually released, bringing a new level of understanding of the inner workings of the counterinsurgents' methods that they can then use to educate their organization. [249] Thus in some ways, detaining members but releasing them prior to the defeat of their organization, makes the organization stronger and more confident through learning and adaptation.[250]

The Principles of Clandestine Cellular Networks

Based on a process-trace analysis of the form, function, and logic of clandestine cellular networks, the survival of a clandestine organization rests on six principles derived from this study of form, function, and logic: compartmentalization, resilience, low signature, purposeful growth, operational risk, and organizational learning (see figure 9). These six principles can be used by the counterinsurgent to analyze current network theories, doctrine, and clandestine adversaries to identify strengths and weaknesses. First, *compartmentalization* comes both from form and function, and protects the organization by reducing the number of individuals with direct knowledge of other members, plans, operations. Compartmentalization provides the proverbial

---

arrested?" Lindsay Moran, *Blowing My Cover: My life as a CIA Spy*, (New York, NY: Penguin Group, 2005), 198-199.

[249] Author's experience with detainees in Iraq. When expected patterns of detention changed, such as the number of days at one detention facility before moving to the next level of detention, the detainees would become visibly upset, realizing that their detention timeline was not normal.

[250] Kyle B. Teamey, "Arresting Insurgency," *Joint Forces Quarterly*, no. 47 (4th quarter 2007): 118, http://www.ndu.edu/inss/Press/jfq_pages/editions/i47/27.pdf [accessed on March 5, 2009]; Woodward, 35. Quoting a Defense Intelligence Agency (DIA) report, Woodward highlights this issue, "insurgents, terrorists, foreign fighters and insurgent leaders captured and released by coalition forces may be more dangerous than they were before being detained."

wall to counter counterinsurgent exploitation and intelligence driven operations. Second, *resilience* comes from organizational form and functional compartmentalization, which not only minimizes damage due to counterinsurgency strikes on the network, but also provides a functional method for re-connecting the network around individuals (nodes) that have been killed or captured. Third is *low signature*, a functional component based on the application of clandestine art or tradecraft, which minimize the signature of communications, movement, inter-network interaction, and operations of the network. *Purposeful growth* is the fourth principle, highlighting the fact that these types of networks do not grow in accordance to modern information network theories, but grow with purpose or aim—to gain access to a target, sanctuary, population, intelligence, or resources.[251] Purposeful growth primarily relies on clandestine means of recruiting new members based on the overall purpose of the network, branch, or cell.

The fifth principle is *operational risk*, which stresses the clandestine paradox between conducting operations to gain or maintain influence, relevance, or reach in order to attain the political goals, and long-term survival of the movement.[252] Operations increase the observable signature of the organization, threatening its survival. The paradox comes in balancing the risk—winning by not losing. It is in these terms that the clandestine cellular networks of the underground develop overt fighting forces—rural and urban—to lethally and non-lethally interact

[251] Naveh, 5.

[252] Molnar, et. al., 6,51.

with the target audiences—the population, the government, the international community, and third party countries conducting foreign internal defense in support of the government forces.[253] This is done to gain moral, physical, and/or cognitive advantage over the counterinsurgents forces and the government by increasing the popular internal support for the movement, as well gain or maintain external support from third party nations or non-state actors. This interaction invariably leads to increased observable signature and counter operations against the insurgent overt elements. However, to balance the paradox of operational risk, these overt elements can, given time and resources, be rebuilt. What cannot be rebuilt are the core members, the driving force behind the insurgency, which can be termed the irreconcilables. These elements stay alive by taking care not to emit any signature that can be detected by the counterinsurgent unless necessary, and making sure that they are compartmented from each other should one be detected.

Lastly, *organizational learning* is the fundamental need to learn and adapt the clandestine cellular network to the current situation, the threat environment, the overall organizational goals and strategy, the relationship with the external support mechanisms, the changing tactics, techniques, and procedures of the counterinsurgents, technology, and terrain—physical, human, and cyber. Although the insurgent core and network leaders, and even members, must continually adapt and learn based on these factors, one of the most important clandestine principles is to learn and adapt based on successes and failures of the form, function, and logic of the clandestine cellular network.[254] Understanding, learning, and adapting to the factors above, including the loss of members, or close calls, allows for the clandestine cellular network to become stronger and

---

[253] Audiences and interaction based on Dr. Gordon McCormick's "Diamond Model"; see Eric P. Wendt, "Strategic Counterinsurgency Modeling," Special Warfare (September 2005), 5.

[254] Otis, 89.

more proficient. Examples of questions that the network leaders and members might ask themselves after any type of attack on the network may include: How did this happen? How did the counterinsurgents find the member? What was he doing when he was detained or killed? Who knew he was at the location? Were there any odd occurrences before the attack? And, what new tactic, technique, or procedures did the counterinsurgent use in executing this strike?[255] All are pertinent questions that may expose an organizational vulnerability that requires the network to adapt.

Thus, much of the logic of clandestine cellular networks emerges from these principles, and all evolve around the often repeated adage, "insurgents win by not losing." It is for this reason that survival of the movement's the core members, or other highly dedicated members that will carry on the fight even if the core is lost, is imperative. These members must remain largely under the counterinsurgent radar by applying the form, function, and logic of clandestine cellular networks for long-term survival. The insurgents may lose the conventional battle, including all of their overt force, but the organization can and will rebuild upon its core, even if it has to wait for a long period of time for the right conditions to re-emerge. Insurgent time and western time are not comparable, nor are the insurgent and western ideas of defeat. Defeat of a conventional fighting force in the past may have meant victory, but for an insurgency, it just means a setback.[256] Defeat against an insurgency also does not come simply by securing the population, as

---

[255] John McLaughlin, "Questions and Answers Highlights" transcript, in *Unrestricted Warfare Symposium 2008*, ed. Ronald R. Luman, (Laurel, MD: John Hopkins University of Applied Physics Laboratory, 2008), 130.

[256] So for example, the combined US and Northern Alliance forces soundly defeated the Taliban's overt fighting force in Afghanistan by December of 2001. Yet, as the Taliban transferred from the "government" of Afghanistan to the insurgent fighting against a US- and NATO-backed Afghan government, over time, the Taliban has rebuilt its overt forces. This growth was based on the efforts of the elements that survived and went underground. They simply faded into the population or crossed the border

US doctrine promotes, although this is the first step.[257] The other steps that must take place include isolating the clandestine networks from external support, and isolating the reconcilable insurgents from the irreconcilables. Until these conditions are satisfactorily met, the fight will continue, maybe not overtly, with subversion and terrorism once again emerging as the primary methods of the latent-and-incipient phase, but it will continue, especially for ideologically motivated individuals. Victory comes for the counterinsurgent only when there are no more irreconcilables, either through turning them, completely isolating and thus marginalizing them, capturing them, or killing them.

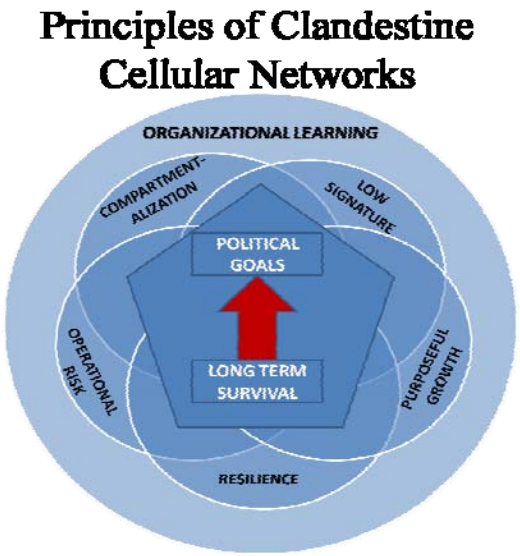

Figure 9. Principles of Clandestine Cellular Networks[258]

---

to sanctuary areas in Pakistan. From 2006 to 2009, the Taliban's overt force has been reconstituted, and transitioned from the latent-insipient phase to the guerrilla warfare phase. In some areas, the Taliban has been successful enough to even transition from the guerrilla warfare phase to the war-of-movement phase where the Taliban controls areas in Afghanistan and conduct large-scale combat operations. Yet, even if all of the Taliban's overt fighting force was defeated today, the Taliban would simply regress back to the latent-incipient phase, and reorganize and rebuild based on the clandestine cellular network that survived.

[257] FM 3-24, 1-29.

[258] Author's figure.

Conclusion and Recommendations

Conclusion

This monograph answered the primary research question—what is the form, function, and logic of clandestine cellular networks? Although each insurgency is unique, underground clandestine cellular networks as the foundation of insurgent organizations are not, nor are their form, function, and logic. Since the dawn of society, clandestine cellular networks have been used to hide nefarious activities within the human terrain. While there has been an increased interest in the use of these types of networks since 9/11, few network theorists or counternetwork theorists and practitioners understand that these networks have a peculiar organizational form, function, and logic. The wrong ontology and epistemology, largely based on mirror-imaging information-age network theories onto clandestine cellular networks, have led many network and network attack theorists astray. This misunderstanding is due to the lack of appreciation for the form, function, and logic of clandestine cellular networks, and ultimately the importance of "organization," one of the seven dynamics of insurgency. Most theorists and practitioners cognitively mirror information-age networks to clandestine cellular networks, which, as this monograph has shown, is largely incorrect. Failure to understand the aspects of clandestine cellular networks has huge implications to both the way network theorists study and model networks, as well as how network attack theorists recommend defeating clandestine cellular networks.

Within the seven dynamics of insurgency, theoretical and doctrinal understanding of the "organization" has been largely focused on the overt military elements of the insurgency, the guerrillas. Throughout history, guerrillas, or the overt military elements of an insurgency, have largely been a rural component, supported by clandestine urban and support components, like the underground and auxiliary, both of which remained largely hidden. For the West, it is easier to understand and identify with the overt military elements, since they are generally organized along

commonly understood military hierarchical formations. Military force can be brought to bear on these elements when they are discovered, although the enemy is still cunning enough to frustrate western military application of force by not seeking decisive military engagements. This is not the case with clandestine elements of an insurgency that require patience and the discriminate use of force to capture or kill.

As the world's societies have migrated into the urban areas, the urban guerrilla, underground, and auxiliaries, all operating as clandestine cellular networks, have become increasingly important, especially the core members of the movement within the underground. The problem from a western military perspective and for the counterinsurgent is that the underground and auxiliary elements, and the urban guerrillas, primarily exist amongst the people, and thus, continually frustrate counterinsurgent operations due to their proximity to the center of gravity for both the insurgent and counterinsurgent—the people. Any misapplication of force by the counterinsurgent automatically delegitimizes the government's efforts.

To further compound this paradox, is the lack of theoretical, doctrinal, and operational understanding of the form, function, and logic of clandestine cellular networks. Since 9/11, the incorrect application of information-age network theories to countering clandestine cellular networks has focused on disconnecting these human networks by attacking key nodes and hubs in an effort to disconnect the network. Although these theories seem intuitive, especially when these network attack methodologies are based on theories designed to disconnect information-age networks, a deeper understanding of the form, function, and logic of clandestine cellular networks reveals that these networks have little in common with information-age networks. By incorrectly focusing on the removal of single, high-value targets—individuals identified based on their key roles, as in the case of leaders, facilitators, financiers, and specially-skilled individuals, or due to their connectivity, such as a highly connected individual or hub, the current network attack methodologies have operated within the tolerance levels of most clandestine cellular networks. The organizational form based on compartmentalization is designed to quickly recuperate from

the removal of individuals, even key individuals. Further, focus on the hubs has effectively "culled the herd" of poor clandestine operators, since these highly connected individuals are violating the most basic principles of clandestine arts or tradecraft, that of maintaining a low signature and minimizing direct contact with other members of the network. Ultimately, the failure to understand form, function, and logic of clandestine cellular networks has led to the application of incorrect methods for countering these networks, leading to a continued failure to truly disrupt, neutralize, defeat, or ultimately destroy the key organizational form that is the bedrock of most insurgencies.

The form, function, and logic construct allows for a greater understanding of clandestine cellular networks. First, form explains the development and interaction of the organizational components of the insurgency—the guerrillas, underground, and auxiliary—specifically focusing on the clandestine components. Further analysis of the clandestine cellular elements reveals that historically, these elements have made up the largest portions of the overall insurgent organization. This monograph also showed that this relationship can be explained in much the same way as conventional military tooth-to-tail ratios, with the guerrilla elements making up only a fraction of the insurgency in comparison to the clandestine elements. This understanding further revealed the overall historical scale of the clandestine networks, based on ideas of network leaders and sub-leaders recruiting and developing their subordinates, a purposeful process that continues with the development of each new leader, resulting in exponential organizational growth. The idea of leaders and subordinates runs counter to many popular theories of leaderless networks as espoused by leading terrorism and insurgency experts.

The investigation of the organizational form also revealed compartmented elements built upon the foundation of the cell. Cells are connected via links to leaders that form branches, sub-networks, and ultimately networks, each with its own function or set of functions, such as leadership, logistics support, intelligence collection, counterintelligence, recruiting, training, finances, information operations, direct action (terrorism, assassination, kidnapping, sabotage,

etc), evasion, shadow government, or support to overt political and military wings. Separating these cells, branches, sub-networks, and network is a method of structure compartmentalization, called a cut-out, which may include no person-to-person contact, or by controlling information—no personal information is known about other cell members, aliases are used, and organizational or operational information is provided to members on a need-to-know basis only. Compartmentalization ultimately protects the organization by limiting the damage done by a counterinsurgent operation should a member of the network be detained or killed. The better the structural compartmentalization, the more limited the damage of any counterinsurgent operation since the direct linkages will end at the cut-out, thus ending the exploitation.

Second, is the organizational function of the clandestine cellular network, which relies on the application of clandestine arts or tradecraft to lower the signature of the members of the network. This is done to allow the network to maintain the lowest signature possible while conducting lethal and non-lethal operations, intelligence collection, logistics support, as well as when members interact, directly or indirectly, to pass information or instructions, to re-connect the network after a member has been killed or captured, and to recruit new members to replace losses or to grow. Organizational growth is conducted with purpose, in an effort to gain access to new human and material resources, targets, or locations for intelligence collection, while functionally limiting the overall risk of bringing new members into the organization. While the initial core members may be family members or trusted friends, all successful insurgencies continue to bring in new members to extend their operational reach. This recruiting includes the recruitment of individuals to operate as a member of the core group, thus requiring significant recruiting efforts and precautions, or individuals that do not have the characteristics of a good

core member, and are simply recruited to operate at the edge of the organization where there is high risk of being killed or captured.[259] The current counternetwork methodologies inadvertently focus on the so-called "low hanging fruit," since they are the most detectable clandestine cellular network elements. This is a bonus for the clandestine leaders near the edge of the organization since they can quickly recruit new cell members, provide them with little clandestine or operational training, since they fully expect these edge elements to be quickly identified once they attack the counterinsurgents. Based on the propensity of most militaries, the clandestine leader further expects these poorly trained cells to draw the counterinsurgent's attention, further protecting the core clandestine members of the network, while giving the counterinsurgents a false sense of success. Regardless of the precautions, interaction between the members is a high-risk endeavor, requiring solid application of clandestine art, or tradecraft to ensure the core members are not detected and linked to others by the counterinsurgent.

Lastly is the overall logic of clandestine cellular networks which ultimately centers on the movement's long-term survival in an effort to reach its political goals; in other words, winning by not losing. The overall purpose of the insurgent movement is long-term survival, relying on the form, function, and logic of clandestine cellular networks to first, minimize the signature of the network to make it difficult for the counterinsurgent to detect, and second, if detected and attacked by the counterinsurgent, to limit the damage. It is also about balancing the need for long-term survival to reach the political goal, while ensuring that the insurgency is active enough to gain or maintain popular internal support and external support. This study has also shown the logic of these networks is based on a worldview where time is relative to the objectives the insurgency seeks, with some core members willing to pursue goals for years and even decades,

[259] Byman, 16-17.

while constantly under the pressure of being killed or captured.[260] It is the clandestine cellular networks that ensure long-term survival of the organization, with the overt military elements being one tool to reach their goal; a tool that given enough time can be replaced if defeated or destroyed. What cannot be replaced is the core movement, those individuals that will carry on the fight despite setbacks, willing to revert to previous phases of the insurgency and wait for better conditions, even if it means waiting for months, years, or decades. This analysis further explained this point by comparing protracted war, military-focused (FOCO), and conspiratorial insurgency theories. Clandestine cellular networks play a significant role in all but the FOCO theory, which is an indicator of the non-viability of this theory given a competent counterinsurgent force and government.

In analyzing the logic, the pressures and stresses of living the clandestine lifestyle were also studied. The pressures of living under constant fear of being killed or captured further separate clandestine cellular networks from information-age networks, such as social and business networking. The pressures alone force the clandestine operators to constantly worry about their application of the form and functions of clandestine cellular networks, a worry that most information-age network members do not face. Ultimately successful counternetwork operations rest on the ability to force the core members to make mistakes by pushing them out of their comfort zones and into carrying out an action that is detectable by the counterinsurgent.[261] This can only be done when the network is not given the opportunity to learn lessons based on the counterinsurgent operations against single individuals or against the poor clandestine operators.

---

[260] Byman, 18-20.

[261] Byman, 104.

Lastly, six clandestine cellular network principles emerged from the process-trace methodology of this study, capturing the essence of the form, function, and logic, and centered on long-term movement survival— compartmentalization, resilience, low signature, purposeful growth, operational risk, and organizational learning. These six principles provide a method for testing network theories for feasibility, acceptability, and suitability, exposing the counterinsurgent to the critical understanding of the most important elements of the insurgency, the clandestine cellular networks as the first step in developing effective counternetwork operations.

Recommendations

First, the US military needs to conduct further research into the form, function, and logic of contemporary insurgencies, specifically those in Iraq, Afghanistan, and globally, focused on al Qaeda and its associated movements. These studies should use the Special Operations Research Office products from the 1960s as a model for these efforts. The author recommends deploying researchers to Iraq and Afghanistan to interview former Sunni and Shi'a insurgents, such as the members of the Sons of Iraq, and detained insurgents, in order to develop an in-depth understanding of the local, as well as al Qaeda and Iranian, methods of clandestine cellular network operations.

Second, include a detailed discussion of the form, function, and logic of clandestine cellular networks, including the underground, auxiliary, and urban guerrillas, in the next version of both the FM 3-24 and the currently draft of joint publication 3-24, to increase the understanding of this organizational form amongst the joint force.

Third, conduct comparative analysis of the form, function, and logic of clandestine cellular networks with current network and network attack methodologies to identify which network theories and network attack methodologies are truly feasible, acceptable, and suitable.

Adjust current counternetwork operations—tactically, operationally, and strategically—based on this analysis.

Appendix A – Types of Clandestine Cellular Networks

Based on the form, function, and the previous elements of logic—goals, decision making, and principles—it becomes obvious that there are different *types* of clandestine cellular networks that are not clearly captured in the form, function, and logic context, but are important to the overall understanding of clandestine cellular networks. This monograph focused on the use of clandestine cellular networks within the framework of an insurgency, both interstate and globally. Three distinguishing aspects of *type* are evident: professional (trained) or non-professional (on-the-job training), indigenous (internal) or non-indigenous (external support), and the relative "clandestine potential" of an insurgency and how an external power can increase this potential. This taxonomy of clandestine cellular networks is largely overlooked or misunderstood by theorists and doctrine. *Professionals* is loosely defined as an individual having some formalized training in conducting clandestine arts or tradecraft, while the *non-professional* has learned the trade through on-the-job training or an evolutionary process—in a sense, "survival of the fittest." This taxonomy also includes a contrast in clandestine capability between the insurgents, which by definition are indigenous to a country, and members of a clandestine, non-indigenous, external support network, either a nation-state or non-state actors. Obviously, nation states have capabilities to conduct espionage against rivals, as well as establishing specially-trained intelligence or military special-operations forces to conduct training, advising, and equipping of insurgencies against rivals as another tool of diplomacy. Although the espionage operations have always been clandestine in nature, the requirement to use clandestine cellular networks to support to insurgency has increased with urbanization, with some countries, such as Iran and its

Intelligence Services (MOIS) and the Iranian Revolutionary Guard Corps (IRGC) efforts against the US in Iraq as a good example of this growing trend.[262]

Non-state actors have now emerged as another type of external support, but to date have largely been confused with the indigenous insurgent elements. Arguably, al Qaeda is the current "gold standard" of non-state actors that use clandestine cellular networks to link like-minded interstate insurgencies, with its global insurgent clandestine cellular network. Al Qaeda as an example, can also be further subdivided into the overall global insurgency movement and special-purpose networks, such as financial networks, intelligence networks, logistics support, and strategic attack networks, such as the closed network that carried out the 9/11 attacks. Thus, the six subcategories of clandestine cellular networks that emerge are: *internal non-professional, internal professional, external professional, external non-professional, non-state clandestine networks, and non-state special purpose cells and networks.* These will be explained in detail below.

First, *internal non-professional clandestine cellular networks* (INP-CCN) consist of insurgents with no formal clandestine training, which is indicative of the grass roots type of insurgency. The non-professionals learn largely from surviving their mistakes or adapting based on their observations of other's successes or failures.[263] There is also the possibility that they have access to military-like training manuals or the internet that provides them access to the theory of

---

[262] See Robert C. Martinage, *The Global War on Terrorism: An Assessment*, (Washington, DC: Center for Strategic and Budget Assessment, 2008), http://www.csbaonline.org/4Publications/PubLibrary/R.20080223.The_Global_War_on_/R.20080223.The_Global_War_on_.pdf [accessed on January 15, 2009]; Cordesman, *Iran's Revolutionary Guards*; Jafarzadeh, *The Iran Threat, Pa*rt III; Robinson, 107, 164,166-167, 342.

[263] Ottis, 129.

clandestine operations.[264] The top tier of this category are those individuals that have received some type of informal clandestine training from a nation-state intelligence, military, or law-enforcement members, likely as an agent of these individuals to gather intelligence. Given these skills, this tier of non-professionals have a distinct advantage and better potential for success through the application of their training to keep the signature of their organization low as it develops and grows.

There is a subset of this first type routinely described as "leaderless jihadists," who start their own grass roots movements based on the ideology of a larger organization, but to which they do not have direct links.[265] As Robert Martinage explains, "Over the past several years, a number of individuals, with distant or no links to al Qaeda and scant terrorist training, have responded to its call to defensive jihad against the West. Inspired by a common cause, these individuals coalesce for a limited campaign or even a single operation."[266]

Second, individuals with some type of formal training in clandestine operations, generally from the intelligence, military, or law enforcement communities develop *internal professional clandestine cellular networks (IP-CCN)*. Having likely been trusted members of the former regime, these types of clandestine operators largely emerge after an authoritarian regime has been overthrown, such as the so-called "former-regime elements" in Iraq. Due to their positions within the security apparatus prior to the overthrow, they likely are still loyal to the previous regime. Thus, they apply their clandestine skills to counter those responsible for the

---

[264] For example see *The Al Qaeda Manual*.

[265] See Sageman, *Leaderless;* Martinage, 28-30.

[266] Martinage, 28.

overthrow.[267] Although beyond the scope of this monograph, this is an important consideration when a regime removal becomes an option for the US and can be termed as a countries "clandestine potential" referring to the built in capacity for the population and security apparatus to use their clandestine skills to develop a large, but hidden clandestine cellular network.[268] These elements could include former military, intelligence or law-enforcement personnel that were trained by the government.[269]

The next two types of networks are both external support networks; one is a nation state network, of made up of intelligence or specially trained military personnel, and the other is an non-state actor network. Both have certain commonalities that must be understood first. Nation-states or non-state actors provide support for insurgency, also known as unconventional warfare, as a low-cost, low-risk, economy of force capability to put pressure on an adversary nation indirectly without having to resort to conventional military methods. Historically, external support provides the insurgency with an increased likelihood of success.[270] There are three types of external support—indirect, direct, and combat.[271] Indirect support consists of political recognition, economic or information support, training outside of the conflict area, or support provided through a third party nation.[272] Direct support would include the previous, but with a more direct relationship, including providing advisors to train, equip, and advise the insurgency, short of combat, and most likely conducted in a sanctuary or liberated area near or within the state

---

[267] Grant, 6.

[268] Clandestine potential is the author's term. Also see Grant, 6.

[269] As one insurgent leader explained to Chehab, "We are all well trained, as most of us took part in the Iran-Iraq War." Chehab, 7.

[270] FM 3-24, 1-6, 1-8, 1-11, 1-15 to 1-17.

[271] Jones, 166-167.

in conflict, respectively.[273] Lastly, combat support would include all of the previously mentioned types of support, but advisors would work directly with the insurgency within the zone of conflict, accepting the risks associated with this type of interaction and proximity, or even direct conflict, with the counterinsurgents.[274] Currently in Iraq, there are two external support entities, the nation-state of Iran, providing indirect and direct support to the Shi'a insurgency, and al Qaeda, a non-state actor, providing indirect, direct, and combat support to the Sunni insurgency, highlighting the differences between the two external support networks—*external non-professional and external professional*.

Third, *external non-professional clandestine cellular networks (ENP-CCN)* inherently define external support to an insurgency by a non-state actor. Al Qaeda's support to like-minded insurgencies is the model for this category.[275] Currently in Iraq, this category is referred to as "foreign fighters and terrorists," which emotionally describes the networks but largely causes them to be lumped together with the insurgency, which by the very nature of insurgency can only consist of indigenous members.[276] Zarqawi and his replacement, Abu Ayyoub Al-Masri, are examples of this non-professional genre.[277] This groups functions much like the US Army Special Forces, providing indirect, direct or combat support to the insurgency, including training, equipping, funding, as well as advising the indigenous insurgent leaders, and if necessary, leading the insurgency. Al Qaeda is a good example of external support gone bad, having suffered from

---

[272] Ibid., 166.

[273] Ibid.

[274] Ibid., 166-167.

[275] Byman, 30-31.

[276] Jeffrey, 4; and Chehab, 37, 43-47.

[277] Jeffrey, 4; see Chehab, 45-62, for an interesting interview with Zarqawi in Iraq.

catastrophic loss of rapport with many Sunni insurgent groups and the Sunni population in 2007. Zarqawi also received harsh criticism from the al Qaeda core, primarily Ayman al-Zawahiri in 2004, for his attacks on the Shi'a population, showing the fine balance that these external support networks must face.[278]

Indirectly, Zarqawi's efforts led to the establishment of recruiting capabilities outside the zone of conflict, and then clandestinely infiltrating these individuals, also referred to as "foreign fighters," using clandestine routes or "rat lines" from Europe and the Middle East into Iraq. These individuals are largely used as suicide bombers, a method of non-state precision attack, more appropriately described as the jihadi direct attack munitions (JDAM).[279] The support networks that infiltrate these individuals and provides support to the al Qaeda elements in Iraq, whether financial or even within the information realm by running al Qaeda websites, including providing cyber-based training materials, are all part of the indirect support provided by the external non-professional network. These networks support the Sunni indigenous networks directly through finances, training, advising, and when necessary organizing and leading. This is generally the role Zarqawi had, not participating directly in combat, but more at the managerial level, working with the leaders of the various insurgent groups to gain consensus and unity of effort. His subordinates conduct combat support to local insurgent movements on a regular basis, and provided training, equipment, finances, advising, and leadership at that level, which included supporting these indigenous units when they engaged in combat. Understanding this allows the counterinsurgency to focus on cutting off external support to deny the insurgents the resources, training, advice, and

---

[278] Jean-Charles Brisard and Damien Martinez, *Zarqawi: The New Face of Al-Qaeda*, (New York, NY: Other Press LLC, 2005), appendix VIII.

[279] This is the author's own terminology based on the US Air Force Joint Direct Attack Munitions (JDAM).

even leadership, provided by these external support networks. The "external non-professional" categorization applies only within the context of interstate insurgency. The clandestine potential of these advisors varies, from very good to very poor, depending largely on how they were trained.

The fourth type of clandestine cellular network is the a nation states' external support networks made up of intelligence personnel and/or special operations forces referred to here as *external professional clandestine cellular networks (EP-CCN)*. This type of support has taken place throughout history. During Napoleon's conquest of Spain between 1808 and 1814, in which the term "guerrilla" was first coined, Napoleon's forces encountered an insurgency supported by the British.[280] Even earlier than this, the British supported the Calabrian brigands in Southern Italy against Napoleon between 1806 and 1811.[281] External support to insurgencies, especially with respect to large numbers of clandestine cellular external support networks reached its peak during World War II when the British Special Operations Executive (SOE) and the American Office of Strategic Services (OSS) provided the largest clandestine efforts in history to support resistance movements throughout occupied Europe and Asia. During the Cold War, external support to insurgency was the primary method of conflict for the super powers, with the Soviet Union and the US both supporting insurgencies throughout the world in attempt to limit the other superpower's influence in the region. Today, the US faces an Iran-backed insurgency in Iraq,

---

[280] John Lawrence Tone, *The Fatal Knot: The Guerrilla War in Navarre and the Defeat of Napoleon in Spain*, (Chapel Hill, NC: The University of North Carolina Press, 1994), 126, 130.

[281] Milton Finley, *The Most Monstrous of Wars: The Napoleonic Guerrilla War in Southern Italy, 1806-1811*, (Columbia: University of South Carolina Press, 1994), 30-33, 71.

where Iran has covertly supported the Shi'a by providing training, funding, and providing lethal aid, largely used to target US forces and force their withdrawal.[282]

The larger clandestine cellular network of al Qaeda, the global insurgency, and other non-state actors can simply be described as *non-state, non-professional clandestine cellular network (NS-NP-CCN),* a fifth category.[283] The difference between this network type and the external non-professional type is in its overarching function. The non-state, non-professional refers to the larger al Qaeda global insurgency movement, while external, non-professional refers to just those non-state networks that are focused on external support of the interstate insurgency. In some cases, these two types may be the same, especially if the external support can be traced to senior leadership in the overarching global insurgency. Although a study of al Qaeda reveals that not only is it a global insurgency that uses and externally supports like-minded insurgencies to further its cause, it also uses special-purpose cells and networks to conduct strategic, direct-action operations against its "near and far enemies."[284] The sixth and final category, the so-called "terrorist cells and network," includes the special-purpose networks, such as the 9/11 hijackers,

---

[282] "Casey emphasized that in recent months there had been an increase in the use of EFPs—explosively formed projectiles—in the Shia areas. He said the technology was coming from Iran and that it was especially lethal;" Woodward, 40.

[283] The use of the double descriptor of "non-state/non-professional" is due to the fact that there may be some non-state, but professionally trained, clandestine networks, such as non-state security firms or corporations that may employ clandestine networks, but are beyond this the scope of this study. Al Qaeda is clearly a non-professional clandestine network as Burton notes, "Poor tradecraft, as history shows, has long been the Achilles' heel of the jihadists and frequently has helped to pre-empt plots. In fact, it could be argued that poor tradecraft has caused the jihadists as much, if not more, grief than have penetrations by the intelligence services that hunt them." Burton provides numerous examples of antics and tradecraft failures of al Qaeda operatives that show the amateurish practices of these elements in stark contrast to a professional nation state intelligence service practice of tradecraft. As he further explains, "combat experience does not necessarily translate into good tradecraft and street skills. Many of the busted operatives discussed [in the article] had combat experience in Afghanistan or Bosnia—and most of them received 'advanced' training at al Qaeda camps in Afghanistan—but they still made significant tradecraft errors." Burton, under "Technical Education vs. Tradecraft" heading.

[284] Byman, 15, 38.

which can be classified as *non-state special-purpose clandestine cellular networks (NS-SP-CCN)*. This category encompasses the cells and networks that carried out the attacks on 9/11 (2001), against the USS Cole (2000), the Tanzania and Nairobi Embassy bombings (1998), and the Mumbai attacks (2008). Although clearly terrorist acts, the "terrorists" themselves were really specially selected and trained individuals chosen for these operations, in much the same way a nation state would choose special operations soldiers. Networks and cells of this type are generally hand-picked by their core-leadership to conduct intelligence gathering, logistics and support operations, and ultimately direct action operations—terrorist acts, ambushes, raids, murder, and hostage taking. What makes this cells different is not only their focused purpose, but also that they are closed networks, which means that they generally are not adding new members.

Although these types of networks may fluctuate in size, they are generally not growing like other networks, since they have a predetermined mission, which require certain skills, logistics support, and intelligence preparation. It is likely that as the mission or network leaders identify a need for special skills or additional support, those elements can be added, and these additions are known and trusted individuals that may or may not know the overall plan. These special-purpose networks and cells are specifically trained, funded, and supported for a certain target. Their mission cycle follows a general pattern of identifying a target that meets the overall effect sought by the core leadership, then developing the intelligence for the target, establishing the support infrastructure for the mission, then attacking the target, and lastly, collapsing the intelligence and support networks once the operation is complete to protect the members for future use. Due to their closed nature, it is very difficult for law enforcement to identify these networks unless they make mistakes that raise their signature. However, if this breach happens, law enforcement has generally been very successful at dismantling these operations quickly. The logic of these clandestine cellular networks is different than other categories, since this is a very mission-focused group that relies heavily on form and function for protection due to the fact that they are operating within a foreign environment. If security forces breach the compartmentalized

and closed network, the entire network is usually exposed and arrested. Members that escape have to assume that the mission is compromised, and thus cancel due to the increased risk, resulting in mission failure.

Complex insurgencies, such as in Iraq and Afghanistan, consist of a mixture of these types of networks and their overt elements. Although, understanding the types of networks present in an active insurgency inform the development of effective counternetwork operation, this same knowledge can inform planners on the types of insurgent threats that may emerge due to US military operations, such as the insurgencies encountered as part of Operation Enduring Freedom and Operation Iraqi Freedom.[285] For this monograph, the capability of an insurgency, both inherent and when supported by external entities, is referred to as *clandestine potential*. This potential is derived by the "type" of networks as just shown—internal or external, professional or non-professional. Each *type* determines the overall likelihood that the insurgent movement will be able to successfully build a core group, underground, and auxiliary, without disruption, upon which is built the overt guerrilla units. The clandestine potential is determined by the network members' experiences, society, and culture, as well as external support capabilities provided by a nation-state or non-state actor in the form of training, advising, and providing resources to increase this potential. Thus, an insurgent movement with members who were former intelligence or military officers trained in clandestine arts would have a greater "clandestine potential" to develop a successful clandestine cellular network than a movement made up of untrained

[285] As Hoffman comments on Operation Iraqi Freedom planning, "The fact that the military planners apparently didn't consider the possibility that sustained and organized resistance could gather momentum and transfer itself into an insurgency reflects a pathology that has long afflicted governments and militaries everywhere: failure not only to recognize the incipient conditions for insurgency, but also to ignore its nascent manifestations and arrest its growth before it is able to gain initial traction and in turn momentum." Hoffman, *Insurgency*, 3.

amateurs who simply take up a cause and learn to operate clandestinely through evolutionary growth based on trial and error, much like on-the-job training. So experientially, school-trained individuals of a nation state's intelligence or military forces would have the requisite skills to clandestinely link into a core of individuals, and begin to grow a clandestine organization, as well as having the understanding on how to apply the principles of clandestine operations to different physical, human, and security environments.

In societies largely controlled by the government through the use of internal, human-intelligence collection networks, as found in authoritarian regimes, there would also be substantial "clandestine potential."[286] In this example, even within a family, members may be intelligence collectors for the government, yet due to their clandestine ability, the family has no idea that they are passing information to an internal security handler. These same skills, as explained in form and function sections in the monograph, apply readily to all clandestine operations, including establishing an insurgency. This potential is further increased if the regime, with its professional intelligence and military elements, has garnered contacts in other sympathetic nations, and can leverage these contacts immediately after being overthrown to provide depth and sanctuaries in other countries, further exacerbating the counterinsurgents' difficulties. A regime worried of being overthrown, may also establish plans for using insurgency as a method of regaining power.[287] Thus, comparing counterinsurgency efforts in Iraq with those in Afghanistan based on clandestine potential, the US military could have identified the clandestine potential in Iraq as a significant threat in the post-conflict operations versus those in

[286] Woodward, 18.

[287] Ibid. Woodward notes that a Defense Intelligence Agency officer that found documents in Iraq showing, "The old regime elements had plans to create a violent, hostile environment."

Afghanistan.[288] Continuing the Iraq example, if this had been identified as an issue, one of the initial tasks would have been to use population-control measures to limit movement and disrupt the ability of these networks from contacting each other clandestinely and developing an underground organization.[289] These networks could also have been attacked early in their underground development as intelligence became available to further disrupt or neutralize their efforts before they were able to move into the guerrilla warfare phase, thus keeping them in a latent or incipient phase of insurgency.

In a country that lacks inherent potential, a third party nation-state or non-state actor may be able to provide training, advising, and equipping either directly, indirectly, or in a combat role to increase the clandestine potential. Normally, this would be difficult and would likely take a long time based on just small special-operations teams or individual intelligence agents slowly increasing the potential over time, as well as organizing a disparate insurgency by providing liaison and establishing relationships between disparate groups being advised by the external support mechanism. However, there is another method for a nation or non-nation state to rapidly increase the "clandestine potential" by infiltrating large numbers of intelligence or military members, or diasporas that have been selected and trained in clandestine operations and

[288] Although there may be a loose correlation, there are other indicators that with further study may solidify this theory, such as the relatively rapid emergence of an insurgency within Iraq, largely clandestine in nature due largely urban insurgency, compared to the insurgency in Afghanistan that has slowly re-emerged since 2001, but was much more rural in nature.

[289] Thus when the Sunni's decided to resist the US occupation, they already had an extensive clandestine competency, and thus could use these skills to coordinate their efforts and build the underground movement under the noses of the US military. The connections with former regime internal security may have also provided a clandestine network frame upon which the former regime internal security elements, now acting as insurgent leaders, could have exploited quickly to link different local insurgent organizations.

conducting insurgency.[290] If they have links to the target country, they are readily accepted back into their homeland, especially at the end of a crisis. ***SDG***

[290] As Jafarzadeh explains, "Since the launch of Operation Iraqi Freedom in 2003, the Iranian regime has provided massive funding, training, and weaponry to militant groups engaged in terrorist activities against coalition forces, has sponsored assassination squads, and has installed a vast espionage network in Iraq. It has brought political influence, manipulated elections, seized control of police departments, and recruited Iraqis into terrorist operations by bribing them with medical aid and other services….The flow of Iranian infiltrators into Iraq grew to staggering proportions by the spring of 2006. Of the 1, 972 foreigners arrested as insurgents between May 2005 and May 2006, 1, 577, or 80 percent, were from Iran." Jafarzadeh, 81.

Bibliography

A Counterintelligence Reader. Edited by Frank J. Rafalko. http://www.fas.org/irp/ops/ci/docs/index.html [accessed March 25, 2009]

Afsar, Shahid, Chris Samples, and Thomas Wood. "The Taliban: An Organizational Analysis." *Military Review* (May-June 2008). http://usacac.army.mil/CAC/milreview/English/MayJun08/SamplesEngMayJun08.pdf [accessed on March 3, 2009].

Andrade, Dale. *Ashes to Ashes: The Phoenix Program and the Vietnam War*. Lexington, MA: Lexington Books, 1990.

Arquilla, John. "It Takes a Network: On Countering Terrorism While Reforming the Military." *Testimony before the House Armed Service Subcommittee on Terrorism, Unconventional Threats and Capabilities*, September 18, 2008. http://armedservices. house.gov/pdfs/TUTC091808/ Arquilla_Testimony091808.pdf [accessed on November 22, 2008].

Arquilla, John, and David Ronfeldt. *In Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica: RAND, 1997. http://www.rand.org/pubs/monograph_reports/MR880/index.html [accessed on November 22, 2008].

_____. *Networks and Netwars*. Santa Monica, CA: RAND, 2001. http:// www.rand.org/pubs/monograph_reports/MR1382/index.html [accessed on January 30, 2009].

_____. *The Advent of NETWAR.* Santa Monica: RAND, 1996. http://www.rand.org/pubs/monograph_reports/MR789/ [accessed on November 22, 2008].

Ashley, Clarence. *CIA Spy Master*. Gretna, LA: Pelican Publishing Company, Inc., 2004.

Associated Press Corps. "Iraqi Forces Weary of America's Troop Withdrawal." *Fox News* Web site. March 09, 2009. http://www.foxnews.com/story/0,2933,507544,00.html [accessed March 9, 2009].

Atkinson, Simon Reay, and James Moffat. *The Agile Organization: From Linear Networks to Complex Effects and Agility.* Washington, D. C.: DoD Command and Control Research Program, July 2005. http://www.dodccrp.org/files/Atkinson_Agile.pdf [accessed January 12, 2009].

Axlerod, Robert, and Michael D Cohen. Harnessing *Complexity: Organizational Implications of a Scientific Frontier*. New York, NY: Basic Books, 2000.

Barnes, Julian E. "Cracking an Insurgent Cell." *U.S. News & World Report* (January 9, 2006). http://www.usnews.com/usnews/news/articles/060109/9military.htm [accessed on November 22, 2008].

Basu, Aparna. "Social Network Analysis of Terrorist Organizations in India." Paper presented at the North American Association for Computational Social and Organizational Science (NAACSOS) Conference 2005, Notre Dame, Indiana, June 26-28, 2005. http://www.casos.cs.cmu.edu/events/conferences /2005/2005_proceedings/Basu.pdf [accessed on November 22, 2008].

Bennett, Andrew, and Alexander L. George. "Process Tracing in Case Study Research." Paper presented at the MacArthur Foundation Workshop on Case Study Methods, Harvard University, Cambridge, MA, October 17-19, 1997. http://users.polisci.wisc.edu/kritzer/teaching/ps816/ProcessTracing.htm [accessed on October 15, 2008].

Bennett, Richard M. *Espionage: Spies and Secrets.* London: Virgin Books Ltd, 2003.

Bertalanffy, L. von. *General Systems Theory*. 5th ed. England: Penguin University Press, 1975.

Birch, David. *The King's Chessboard*. New York, NY: Puffin Books, July 1993.

Borgatti, Stephen P. "Identifying Sets of Structurally Key Players." Lecture, Carnegie Mellon University Center for Computational Analysis of Social and Organizational Systems (CASOS), June 21, 2002. http://www.casos.cs.cmu.edu/publications/papers/CASOSConf_2002_Day1.pdf [accessed November 22, 2008].

_____. "Identifying sets of key players in a social network." Computational & Mathematical Organizational Theory 12 (October 2006): 21, 30. http://www.analytictech. com/borgatti/papers/ cmotkeyplayer.pdf [accessed January 15, 2009].

Bowden, Mark. "The Ploy." *The Atlantic* (May 2008): 4. http://www.theatlantic.com/doc/200705/tracking-zarqawi [accessed November 28, 2008].

Brafman, Ori and Rod A. Beckstrom. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York, NY: Penguin Group, 2006.

Brisard, Jean-Charles, and Damien Martinez. *Zarqawi: The New Face of Al-Qaeda*. New York, NY: Other Press LLC, 2005.

Buchanan, Mark. *Nexus: Small Worlds and the Groundbreaking Science of Networks*. New York, NY: W. W. Norton & Company, Inc., 2002.

Bunker, Robert J. ed. *Networks, Terrorism and Global Insurgency*. New York: Routledge Taylor&Francis Group, 2005.

Burton, Fred. "Beware of 'Kramer': Tradecraft and the New Jihadists." *STRATFOR* (January 19, 2006). http://www.stratfor.com/beware_kramer_tradecraft_and_new_jihadists [accessed on November 16, 2008].

Byman, Daniel. The *Five Front War: The Better Way to Fight Global Jihad*. Hoboken, NJ: John Wiley & Sons, 2008.

Carley, Katlheen, Jeffrey Reminga and Natasha Kamneva. "Destabilizing Terrorist Networks," NAACSOS Conference Proceedings. Pittsburgh, PA, 2003.

Carley, Kathleen M. *Estimating Vulnerabilities in Large Covert Networks*. Pittsburgh, PA: Carnegie Mellon University, Institute for Software Research International, June 2004. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA466095&Location=U2&doc=GetTRDoc.pdf [accessed November 22, 2008].

Chehab, Zaki. *Inside the Resistance: The Iraqi Insurgency and the Future of the Middle East*. New York, NY: Nation Books, 2005.

Cordesman, Anthony H. *Iraq's Sunni Insurgents: Looking Beyond Al Qa'ida*. Working draft, Washington, D.C.: Center for Strategic and International Studies, July 16, 2007, http://www.csis.org/ media/csis/pubs/070716_sunni_insurgents.pdf [accessed on February 8, 2009].

_____. *Iran's Revolutionary Guards, the Al Quds Force, and Other Intelligence and Paramilitary Forces*. Rough working draft, Washington, D.C.: Center for Strategic and International Studies, July 16, 2007. http://www.csis.org/media/csis/pubs/070816_cordesman_report.pdf [accessed on February 8, 2009].

Deleuze, Gilles and Felix Guattari. *A Thousand Plateaus; Capitalism and Schizophrenia*. Minneapolis: University of Minnesota Press, 1987.

Department of the Army. Field Manual 3-05.130, *Army Special Operations Forces Unconventional Warfare*. Washington, DC: US Government Printing Office, September 2008.

_____. Field Manual 3-05.201, *Special Forces Unconventional Warfare Operations*. Washington, DC: US Government Printings Office, April 30, 2003.

_____. Field Manual 3-24, *Counterinsurgency*. Washington, D.C.: U.S. Government Printing Office, December 2006.

_____. Field Manual 31-20-3, *Foreign Internal Defense: Tactics, Techniques, and Procedures for Special Forces*. Washington, D.C.: US Government Printings Office, September 20, 1994.

_____. Field Manual 90-8, *Counterguerrilla Operations*. Washington, D.C.: U.S. Government Printing Office, August 1986. http://www.globalsecurity.org/military /library/policy/army/fm/90-8/index.html [accessed October 7, 2008].

_____. Pamphlet No. 550-104, *Human Factors Considerations of Undergrounds in Insurgencies*. Washington, DC: Headquarters, Department of the Army, September 1966. http://cgsc.cdmhost.com/cgi-bin/showfile.exe?CISOROOT= /p4013coll9&CISOPTR=85 [accessed on November 22, 2008].

Department of Defense. *Commander's Handbook for an Effects-Based Approach to Joint Operations*. Suffolk, VA: US Joint Forces Command, February 24, 2006. http:// accsco.be/wp-content/download/5%20-USJFCOM%20-%20%20Commanders %20Handbook%20for%20an%20Effects-Based%20Approach%20to% 20Joint%20 Operations%20.pdf [accessed on November 22, 2008].

_____. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, (Washington, D.C.: Government Printing Office, amended October 1, 2008), http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf [accessed on November 22, 2008].

_____. Joint Publication 3-0, *Operations*. Washington, DC: Government Printing Office, 13 February 2008. http://www.fas.org/irp/doddir/dod/jp3_0.pdf [accessed on November 22, 2008].

Di Justo, Patrick. "How Al-Qaida Site Was Hijacked," *WIRED* (August 10, 2002). http://www.wired.com/culture/lifestyle/news/2002/08/54455 [accessed March 7, 2009].

Dombroski, Matthew J., and Kathleen Carley, "NETEST: Estimating a Terrorist Network's Structure," (lecture, Carnegie Mellon University Center for Computational Analysis of Social and Organizational Systems (CASOS), June 21, 2002), http://www.casos. cs.cmu.edu/publications/ papers/CASOSConf_2002_Day1.pdf [accessed November 22, 2008],13-16.

Downs, Doneda. *Gauging the Commitment of Clandestine Members*. MS Thesis, AFIT/GOR/ENS/06M-06. School of Engineering and Management, Air Force Institute of Technology (AU), Wright Patterson, OH, March 2006.

Dulles, Allen W. *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World.* Guilford, CT: The Lyons Press, 2006.

Falleti, Tulia G "Theory-Guided Process-Tracing in Comparative Politics: Something Old, Something New." *Newsletter of the Organized Section in Comparative Politics of the American Political Science Association* 17, no. 1 (Winter 2006): 9-14.

http://www.polisci.upenn.edu/~falleti/Falleti-CP-APSANewsletter06-TGPT.pdf [accessed on November 28, 2008].

Fivecoat, David G., and Aaron T. Schwengler. "Revisiting *Modern Warfare*: Counterinsurgency in the Mada'in Qada." *Military Review* (November-December 2008): 77-87 http://usacac.army.mil/CAC2/MilitaryReview/ Archives/English/MilitaryReview _20081231_art012.pdf [accessed on March 2, 2009].

Foot, M.R.D. *SOE: The Special Operations Executive 1940-46*. N.P.: University Publications of America, Inc., 1986.

Freeman, Linton C. "Centrality in Social Networks: Conceptual Clarification," *Social Networks*,1:215-239, 1978.

Galula, David. *Counterinsurgency Warfare: Theory and Practice*. St. Petersburg, FL: Hailer Publishing, 2005.

Garfinkel, Simson L. "Leaderless resistance today." *First Monday* 8, no. 3 (March 2003): under "An introduction to leaderless resistance." http://firstmonday.org/issues/issue8_3/ garfinkel/ index.html [accessed on January 8, 2009].

Godson, Roy. *Dirty Tricks or Trump Cards: U.S. Covert Action & Counterintelligence*. New Brunswick, NJ: Transaction Publishers, 2004.

Gompert, David C. *Heads We Win: The Cognitive Side of Counterinsurgency (COIN)*. Santa Monica, CA: RAND Corporation, 2007. http://www.rand.org/pubs/occasional_papers/ 2007/RAND_OP168.pdf [accessed on March 4, 2009].

_____. "U.S. Should Take Advantage of Improved Security in Iraq to Withdraw." *San Francisco Chronicle* (December 2, 2007). http://www.rand.org/commentary/2007/ 12/02/SFC.html [accessed on November 10, 2008].

Gordon, Michael R. and Bernard E. Trainor. *Cobra II: The Inside Story of the Invasion and Occupation of Iraq*. New York, NY: Pantheon Books, 2006.

Grant, Greg. "Insurgency Chess Match: Allies Match Wits, Tactics with Ever-Changing Enemy in Iraq." *Defense News* (February 27, 2006): 6.

Gunaratna, Rohan. *Inside Al Qaeda: Global Network of Terror*. New York, NY: The Berkley Publishing Group, June 2003.

Hatch, Mary Jo. *Organization Theory*. Oxford, England: Oxford University Press, 1997.

Hayward, Edward PW. *Planning Beyond Tactics: Towards a Military Application of the Philosophy of Design in the Formulation of Strategy*. Master's thesis, Fort Leavenworth, KS, 2008. http://usacac.army.mil/cac2/ SAMS/ HaywardMonograph-PhilosophyofDesign.pdf [accessed on March 2, 2009].

Hoffman, Bruce and Jennifer Morrison Taw. *A Strategic Framework for Countering Terrorism and Insurgency*. Santa Monica: RAND, 1998.

Hoffman, Bruce. *Insurgency and Counterinsurgency in Iraq*. Santa Monica, CA: RAND Corporation, 2004. http://www.rand.org/pubs/occasional_papers/2005/ RAND_OP127.pdf [accessed on November 22, 2008].

_____. "Combating Al Qaeda and the Militant Islamic Threat." Testimony presented to the House Armed Service Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities, February 16, 2009. Santa Monica, CA: RAND Corporation, 2006).

http://www.rand.org/ pubs/testimonies/2006/ RAND_CT255.pdf [Accessed January 15, 2009].

Holme, Petter, Boem Jun Kim, Chang No Yoon, and Seung Kee Han. "Attack vulnerability of complex networks." *Physical Review* E 65 (2002): 12. http://nlsc.ustc.edu.cn/ BJKim/PAPER/ PhysRevE_65_056109%20Attack%20 vulnerability%20of%20 complex%20networks.pdf [accessed January 30, 2009].

Irwin, Will. *The Jedburghs: The Secret History of the Allied Special Forces, France 1944.* New York, NY: Public Affairs, 2005.

Jafarzadeh, Alireza . *The Iran Threat: President Ahmadinejad and the Coming Nuclear Crisis.* New York, NY: Palgrave MacMillan, 2007.

Janis, Irving L. and Leon Mann. *Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment*. New York, NY: The Free Press, 1977.

Jones, D. *Ending the Debate: Unconventional Warfare, Foreign Internal Defense, and Why Words Matter*. Master's thesis, Fort Leavenworth, 2006. http://cgsc.cdmhost.com/cgi-bin/showfile.exe?CISOROOT=/p4013coll2&CISOPTR=554&filename=555.pdf [accessed on December 21, 2008].

Jones, Seth G. and Martin C. Libicki. *How Terrorist Groups End: Lessons from Countering al Qa'ida*. Santa Monica, CA: RAND Corporation, 2008. http://www.rand.org/pubs/ monographs/2008/RAND_MG741-1.pdf [accessed on March 23, 2009],

Karski, Jan. *The Story of a Secret State*. Boston: Houghton, Mifflin Co., 1944.

Kitson, Frank. *Low Intensity Operations: Subversion, Insurgency, and Peacekeeping*. St. Petersburg, FL: Hailer Publishing, no date.

Klein, Gary. *Sources of Power: How People Make Decisions*. Cambridge, MA: MIT Press, 1999.

Krebs, Valdis E. "Uncloaking Terrorist Networks." *First Monday* 7, no. 4 (April 1, 2002). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/941/863 [accessed on November 22, 2008].

Langdon, Lisa, Alexander J. Sarapu, and Matthew Wells. "Targeting the leadership of terrorist and insurgent movements: Historical Lessons for Contemporary Policy Makers." *Journal of Public and International Affairs* 15 (Spring 2004). http://www.princeton.edu/~jpia/ pdf2004/Chapter%204.pdf [accessed on 23 March 2009].

La Porte, Todd R., ed. *Organized Social Complexity: Challenge to Politics and Policy*. Princeton University Press, 1975.

Manheim, Jarol B., Richard C. Rich, Lars Willnat, and Craig L. Brians. *Empirical Political Analysis*. 6th Edition. New York: Longman Publishers.

Mao Tse-Tung, *On the Protracted War*. Peking, China: Foreign Languages Press, 1967.

McCuen, John J. *The Art of Counter-Revolutionary War*. St. Petersburg, FL: Hailer Publishing, 2005.

McGrath, John J. *The Other End of the Spear: The Tooth-to-Tail Ratio (T3R) in Modern Military Operations*. The Long War Series Occasional Paper 23. Fort Leavenworth, KS: Combat Studies Institute Press, 2007.

McLaughlin, John. "Questions and Answers Highlights." Transcript, in *Unrestricted Warfare Symposium 2008*. Edited by Ronald R. Luman. Laurel, MD: John Hopkins University of Applied Physics Laboratory, 2008.

Miksche, F.O. *Secret Forces: The Technique of Underground Movements*. London: Faber and Faber Limited, 1950.

Miller, Russell. *Behind The Lines: The Oral History of Special Operations in World War II*. New York, NY: New American Library, 2002.

Mitchell, Richard P. *The Society of the Muslim Brotherhood*. New York, NY: Oxford University Press, 1993.

Molnar, Andrew R., William A Lybrand, Lorna Hahn, James L. Kirkman, and Peter B. Riddleberger. *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare*. Washington, DC: Special Operations Research Office, November 1963. http://handle.dtic.mil/100.2/AD436353 [accessed on December 21, 2008].

Momboisse, Raymond M. *Blueprint of Revolution: The Rebel, The Party, The Technique of Revolt*. Springfield, IL: Charles C Thomas, 1970.

Moran, Lindsay. *Blowing My Cover: My life as a CIA Spy*. New York, NY: Penguin Group, 2005.

Motter, Adilson E. and Ying-Cheng Lai, "Cascade-based attacks on complex networks," *Physical Review* E 66, (December 20, 2002): 1-4, http://chaos1.la.asu.edu/~yclai/papers/PRE_02_ML_3.pdf [accessed March 4, 2002.

Nance, Malcolm W. *Terrorist Recognition Handbook: Practitioner's Manual for Predicting and Identifying Terrorist Activities*. 2nd ed. Boca Raton, FL: CRC Press, Taylor & Francis Group, 2008.

National Security Council. *National Strategy for Combating Terrorism*. Washington, D.C.: The White House, 2006. http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/nss2006.pdf [accessed April 6, 2009].

Naveh, Shimon. *In Pursuit of Military Excellence: the Evolution of Operational Theory*. Portland, OR: Frank Cass Publishers, 2000.

Ney, Virgil. *Guerrilla War: Principles and Practices*. Washington, D.C.: Command Publications, 1961.

O'Neill, Bard E. *Insurgency & Terrorism: From Revolution to Apocalypse*. 2nd ed. Washington, D.C.: Potomac Books, 2005.

Orlov, Alexander. *Handbook of Intelligence and Guerrilla Warfare*. An Arbor: The University of Michigan Press, 1965.

Ottis, Sherri Greene. *Silent Heroes: Downed Airmen and the French Underground*. Lexington, KY: The University Press of Kentucky, 2001.

Owen, Mark. *A Discussion of Covert Channels and Steganography*. N.p.: SANS Institute, March 19, 2002. http://www.sans.org/reading_room/whitepapers/ covert/a_discussion_of_ covert_channels_and_steganography_678?show= 678.php&cat=covert [accessed on March 5, 2009].

Pillar, Paul R. *Terrorism and U.S. Foreign Policy*. Washington, D.C.: The Brookings Institution, 2003.

Prikhodko, I.E. *Characteristics of Agent Communications and of Agent Handling in the United States of America*. San Francisco, CA: Interservice Publishing Company, Inc., 1981.

Robinson, Linda. *Tell Me How This Ends*. New York, NY: PublicAffairs, 2008.

Roy, Roger. “Tracking down Afghan insurgents like a “chess game” for U.S. troops.” *The Seattle Times*. November 28, 2005. http://seattletimes.nwsource.com/cgi-bin/PrintStory.pl?document_id=2002650678& zsection_id=2002107549&slug= afghanenemy28&date=20051128 [accessed on March 19, 2009].

Ryan, Henry Butterfield. *The Fall of Che Guevara: A Story of Soldiers, Spies, and Diplomats*, New York, NY: Oxford University Press, 1998.

Sageman, Marc. *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia, PA: University of Pennsylvania Press, 2008.

_____. *Understanding Terror Networks.* Philadelphia: University of Pennsylvania Press, 2004.

Sheehan, Michael A. *Crush the Cell: How to Defeat Terrorism without Terrorizing Ourselves.* New York: Crown Publishers, 2008.

Simpson Charles M., III. *Inside the Green Berets: The First Thirty Years*. Novato, CA: Presidio Press, 1983.

SPOOK86 [pseud.]. “The Tape Zawahiri Had to Release.” In From the Cold, formerspook.blogspot. Entry posted January 31, 2006. http://formerspook.blogspot.com/ 2006/01/tape-zawahiri-had-to-release.html [accessed on January 24, 2009].

Spulak, Robert G. Jr., and Jessica Glicken Turnley. *Theoretical Perspectives of Terrorist Enemies as Networks*. JSOU Report 05-03. Hulburt Field, FL: Joint Special Operations University, OCT 2005.

Taber, Robert. *The War of the Flea: A Study of Guerrilla Warfare Theory and Practice*. New York, NY: Lyle Stuart, Inc., 1965.

Teamey, Kyle B. “Arresting Insurgency.” *Joint Forces Quarterly*, no. 47, (4th quarter 2007): 117-122. http://www.ndu.edu/inss/Press/jfq_pages/editions/i47/27.pdf [accessed on March 5, 2009].

Thani, Jumada al-, trans. “Letter from al-Zawahiri to al-Zarqawi.” *GlobalSecurity.org*. July 9, 2005. http://www.globalsecurity.org/security/library/report/2005/zawahiri-zarqawi-letter_9jul2005.htm [accessed January 19, 2009].

The Al Qaeda Manual. Translated by the Manchester (England) Metropolitan Police. No other publication data. http://www.au.af.mil/au/ awc/ awcgate/terrorism/alqaida_manual/ manualpart1_1.pdf [Accessed November 24, 2008].

“The King’s Chessboard Solution.” http://educ.queensu.ca/~fmc/ march2003/ KingsChessboardSoln.html [accessed on March 5, 2009].

Thompson, Robert. *Defeating Communist Insurgency: Experiences from Malaya and Vietnam*. London: Chatto & Windus, 1974.

Tovo, Ken. “From the Ashes of the Phoenix: Lessons for Contemporary Counterinsurgency Operations.” In *Strategic Challenges for Counterinsurgency and the Global War on Terrorism*, 17-42. Edited by Williamson Murray. Carlisle, PA: Strategic Studies Institute, September 2006. http://www.strategicstudiesinstitute.army.mil/ pdffiles/PUB710.pdf [accessed on March 5, 2009].

Trinquier, Roger. *Modern Warfare: A French View of Counterinsurgency*. Translated by Daniel Lee, (London: Pall Mall Press, 1964), http://cgsc.leavenworth.army.mil/carl/resources/ csi/trinquier/trinquier.asp [accessed January 15, 2009].

Tsvetovat, Maksim, and Kathleen M. Carley. “Bouncing Back: Recovery Mechanisms of Covert Networks,” Paper presented at the *NAACSOS Conference 2003*, Day 3, Pittsburgh, PA, June 2003. http://www.casos.cs.cmu.edu/publications/papers/tsvetovat_2003_bouncingback.pdf [accessed November 22, 2008].

Tucker, David and Christopher J. Lamb, *United States Special Operations Forces*, (New York, NY: Columbia University Press, 2007), 208-209.

Turbiville, Graham H., Jr. *Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations: Selected Perspectives and Experience*. Joint Special Operations University Report 07-6. Hurlburt Field, FL: Joint Special Operations University, June 2007. http://jsoupublic.socom.mil/publications/jsou/ JSOU07-6turbivilleHuntingLeadershipTargets_final.pdf [accessed on November 22, 2008].

U.S. Government Counterinsurgency Guide. Washington, D.C.: Bureau of Political-Military Affairs, 2009. www.state.gov/t/pm/ppa/pmppt [accessed March 25, 2009].

United States Military Assistance Command. *PHUNG HOANG Advisors Handbook*. Vietnam: United States Military Command, November 20, 1970. http://www.virtual.vietnam.ttu.edu/cgi-bin/starfetch.exe?cjGDEhjqEBDExu9fCcjH5b3 O7WlKcAYxLC5Cpx3X@VJlyYEeHvEd5qSHNUIJ43IL6ur4w9KL5VsJ2XIamvRZFwD1ESf@IDwdrC4x8S60DoE/1370406001.pdf [accessed on March 25, 2009].

Von Dach Bern, H. Total Resistance: Swiss Army Guide to Guerrilla Warfare and Underground Operations. Edited by R. K. Brown. Boulder, CO: Panther Publications, Inc., 1965.

Ward, Robert J., “Oil Spot: Spreading Security to Counter Insurgency” *Special Warfare* 20, no.2 (March-April 2007): 8-17. http://www.soc.mil/swcs/swmag/07Mar.pdf [accessed on March 2, 2009].

Wendt, Eric P. “Strategic Counterinsurgency Modeling.” *Special Warfare* 18, no. 2 (September 2005): 2-13. http://www.soc.mil/swcs/swmag/05sep.pdf [accessed on March 2, 2009].

West, Simon, Mike Stenson, Chad Oman, and Branko Lustig, “Scene 5,” *Black Hawk Down*, DVD, directed by Ridley Scott, Culver City, CA: Columbia Pictures, 2002.

White, Jeffrey. *An Adaptive Insurgency: Confronting Adversary Networks in Iraq*. Policy Focus #58. Washington, D.C.: The Washington Institute for Near East Policy, September 2006. http://www.washingtoninstitute.org/pubPDFs/PolicyFocus58.pdf [accessed on March 23, 2009].

Windrem, Robert. “Where is Osama Bin Laden? An analysis.” *Deep Backgound: NBC News Investigates*. June 13, 2008. http://deepbackground.msnbc.msn.com/archive/2008/06/13/1138296.aspx [accessed on January 22, 2009].

Wingate, Jim. *The Perfect Dead Drop: The Use of Cyberspace for Covert Communications*. West Virginia: Steganography Analysis and Research Center, n.d. http://www.infosec-technologies.com/steganograph.pdf [accessed March 5, 2009].

Woodward, Bob. *The War Within: A Secret White House History 2006-2008*. New York, NY: Simon & Schuster, 2008.

Zanini, Michele, and Sean J.A. Edwards. “The Networking of Terror in the Information Age.” In *Networks and Netwars*, ed. John Arquilla and David Ronfeldt. (Santa Monica, CA: RAND, 2001). http://www.rand.org/pubs/monograph_reports/MR1382/index.html [accessed on January 30, 2009].

Zayyat, Montasser al-. *The Road to Al-Qaeda: The Story of Bin Lāden's Right-Hand Man.* Edited by Sara Nimis. Tranlated by Ahmed Fekry. Sterling, VA: Pluto Press, 2004.